WEB ACCESS

So i was doing a misc challenge in the CTF and found Web_access to be an interesting one it stated

“simple analysis is required.”

What type of analysis?

So i started with downloading the file called web_access and checked its file type by

-> file web_access

```
└─$ file web_access
web_access: Zip archive data, at least v2.0 to extract, compression method=deflate
```

So now we know its a zip file ready to be unzipped so we used

-> unzip web_access -d web_access_ctf

Into a directory called web_access_ctf but it asked for a password prompt

```
└─$ unzip web_access -d web_access_ctf
Archive:  web_access
[web_access] web_access.log password:
```

Since it had no other clue as to what the password could be so the best approach i thought was to brute force it using john and fcrackzip

```
└─$ fcrackzip -u -D -p foxlist.txt web_access

PASSWORD FOUND!!!!: pw == thequickbrownfoxjumpsoverthelazydog
```

Found it!!! After finding the password we can now open the zip to see whats inside

```
└─$ unzip web_access -d web_access_ctf
Archive:  web_access
[web_access] web_access.log password:
  inflating: web_access_ctf/web_access.log
```

So what the description said was this we have to analyze this log

It was a 50k lines log input searching the flag in it was impossible so i tried opening it and just by opening it i found a pattern

```
109 192.168.0.14 - - [24/11/2024:18:04:48 +0000] "POST /contact HTTP/1.1" 500 2189 "http://example.com" "Safari/537.36"
110 192.168.0.105 - - [19/12/2024:03:39:17 +0000] "GET /login HTTP/1.1" 200 1787 "http://test.com" "Safari/537.36"
111 192.168.0.53 - - [22/06/2024:14:01:55 +0000] "POST /contact HTTP/1.1" 500 311 "http://example.com" "Safari/537.36"
112 192.168.0.222 - - [24/11/2024:07:41:32 +0000] "POST /index.html HTTP/2" 500 2553 "http://test.com" "Mozilla/5.0"
113 192.168.0.82 - - [14/01/2024:13:59:36 +0000] "POST /admin HTTP/1.1" 200 410 "http://example.com" "Safari/537.36"
114 192.168.0.188 - - [01/07/2024:20:29:36 +0000] "GET /admin HTTP/2" 500 1526 "-" "Safari/537.36"
115 192.168.0.67 - - [13/07/2024:06:33:09 +0000] "GET /index.html HTTP/1.1" 500 2933 "http://test.com" "Mozilla/5.0"
116 192.168.0.92 - - [10/02/2024:01:32:28 +0000] "GET /search?id=1' OR SUBSTRING((SELECT f),1,1)='f' --  HTTP/2" 200 894 "-" "Safari/537.36"
117 192.168.0.241 - - [04/12/2024:21:02:37 +0000] "POST /products HTTP/2" 200 2787 "-" "Mozilla/5.0"
118 192.168.0.107 - - [14/05/2024:19:20:47 +0000] "GET /login HTTP/2" 404 3939 "http://test.com" "Safari/537.36"
119 192.168.0.87 - - [19/05/2024:09:44:40 +0000] "POST /admin HTTP/1.1" 200 597 "-" "Mozilla/5.0"
120 192.168.0.114 - - [27/09/2024:01:28:28 +0000] "POST /contact HTTP/2" 404 3778 "http://example.com" "Chrome/91.0"
121 192.168.0.187 - - [23/05/2024:23:11:01 +0000] "POST /products HTTP/1.1" 500 4275 "-" "Mozilla/5.0"
122 192.168.0.216 - - [03/10/2024:15:07:50 +0000] "POST /login HTTP/1.1" 200 4978 "http://example.com" "Safari/537.36"
123 192.168.0.10 - - [28/10/2024:15:33:21 +0000] "POST /index.html HTTP/2" 404 2398 "http://example.com" "Chrome/91.0"
124 192.168.0.217 - - [08/10/2024:12:27:07 +0000] "POST /products HTTP/2" 404 1207 "http://example.com" "Mozilla/5.0"
125 192.168.0.19 - - [24/10/2024:11:20:26 +0000] "POST /index.html HTTP/2" 500 3082 "http://example.com" "Mozilla/5.0"
126 192.168.0.225 - - [24/01/2024:11:03:44 +0000] "GET /admin HTTP/1.1" 403 2481 "http://test.com" "Mozilla/5.0"
127 192.168.0.167 - - [23/04/2024:18:13:37 +0000] "GET /products HTTP/2" 403 4136 "-" "Safari/537.36"
128 192.168.0.149 - - [22/01/2024:19:40:05 +0000] "POST /contact HTTP/1.1" 200 4247 "http://test.com" "Mozilla/5.0"
```

```
314 192.168.0.5 - - [06/01/2024:04:10:14 +0000] "POST /admin HTTP/2" 200 2056 "http://test.com" "Safari/537.36"
315 192.168.0.146 - - [25/09/2024:05:11:37 +0000] "GET /products HTTP/1.1" 200 1717 "-" "Chrome/91.0"
316 192.168.0.199 - - [23/07/2024:21:45:12 +0000] "GET /login HTTP/2" 200 2021 "http://test.com" "Chrome/91.0"
317 192.168.0.31 - - [28/02/2024:16:00:04 +0000] "POST /admin HTTP/2" 200 4170 "http://test.com" "Safari/537.36"
318 192.168.0.24 - - [18/10/2024:09:06:07 +0000] "POST /index.html HTTP/1.1" 404 1634 "-" "Chrome/91.0"
319 192.168.0.193 - - [24/03/2024:14:09:31 +0000] "POST /login HTTP/2" 404 2891 "http://example.com" "Mozilla/5.0"
320 192.168.0.55 - - [16/01/2024:11:39:39 +0000] "POST /admin HTTP/1.1" 404 4940 "http://test.com" "Chrome/91.0"
321 192.168.0.198 - - [09/04/2024:02:29:55 +0000] "GET /search?id=1' OR SUBSTRING((SELECT l),1,1)='l' --  HTTP/2" 403 4945 "-" "Chrome/91.0"
322 192.168.0.25 - - [07/12/2024:03:18:03 +0000] "POST /products HTTP/2" 200 4904 "http://test.com" "Safari/537.36"
323 192.168.0.65 - - [15/01/2024:02:54:08 +0000] "POST /products HTTP/2" 404 4907 "http://test.com" "Mozilla/5.0"
324 192.168.0.41 - - [24/03/2024:21:21:46 +0000] "GET /index.html HTTP/2" 500 4649 "http://example.com" "Chrome/91.0"
325 192.168.0.251 - - [21/01/2024:02:58:36 +0000] "GET /contact HTTP/1.1" 403 4850 "http://example.com" "Safari/537.36"
326 192.168.0.249 - - [19/11/2024:22:52:05 +0000] "GET /index.html HTTP/1.1" 200 5000 "http://test.com" "Chrome/91.0"
327 192.168.0.6 - - [14/03/2024:15:48:36 +0000] "POST /contact HTTP/2" 403 2726 "-" "Mozilla/5.0"
328 192.168.0.96 - - [14/09/2024:21:17:08 +0000] "POST /index.html HTTP/1.1" 403 897 "http://test.com" "Safari/537.36"
329 192.168.0.163 - - [12/08/2024:03:13:52 +0000] "POST /products HTTP/1.1" 500 4866 "http://example.com" "Mozilla/5.0"
330 192.168.0.102 - - [13/12/2024:08:41:22 +0000] "GET /products HTTP/1.1" 404 3535 "-" "Mozilla/5.0"
331 192.168.0.144 - - [18/07/2024:19:15:53 +0000] "POST /admin HTTP/1.1" 500 1870 "http://test.com" "Mozilla/5.0"
332 192.168.0.214 - - [22/06/2024:17:28:46 +0000] "POST /contact HTTP/2" 403 4330 "http://example.com" "Chrome/91.0"
```

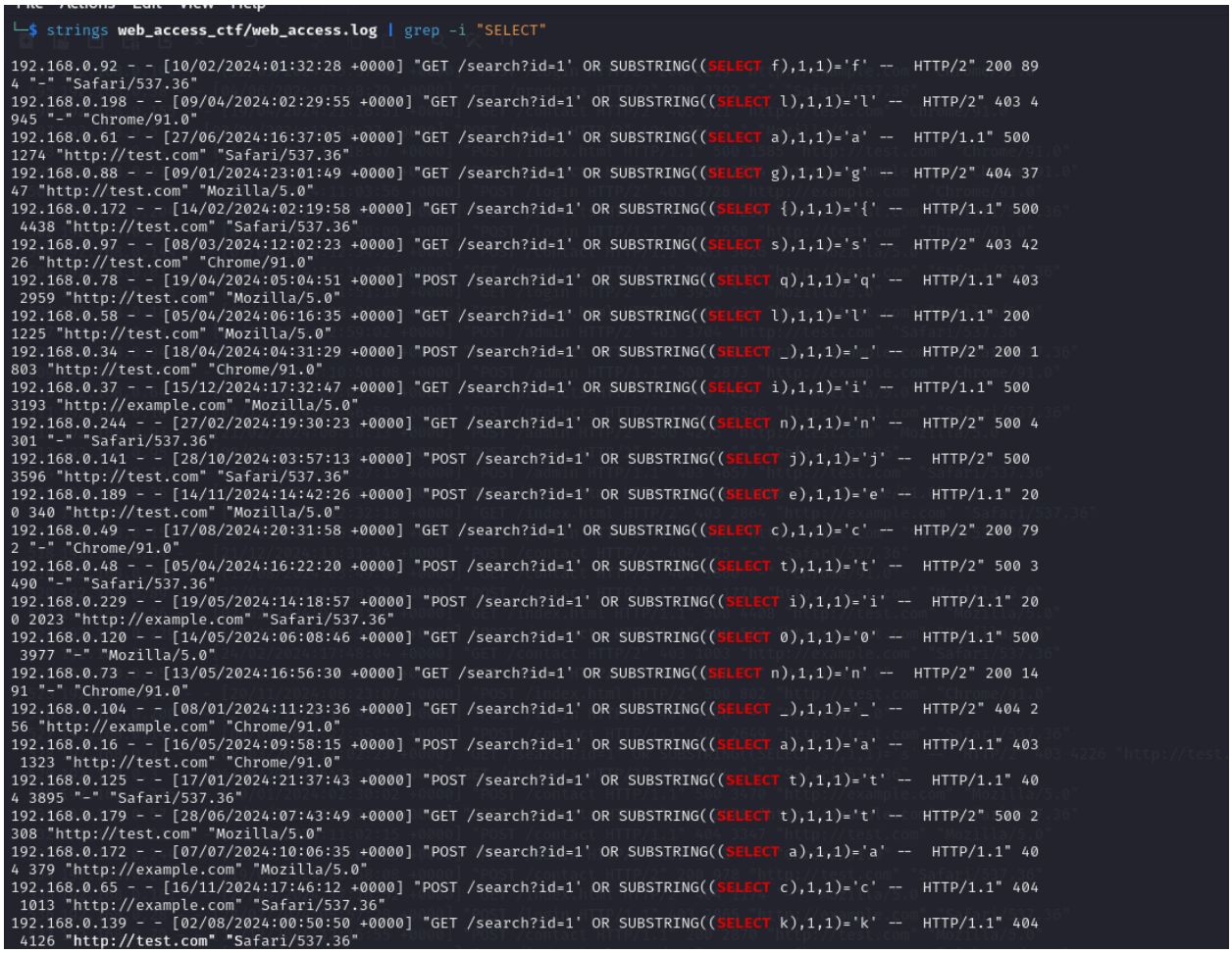
You see those long string?? They have something like f and l

```
941 "http://examp
1 "http://example
G((SELECT a),1,1)=
37 "http://test.c
```

Upon inspecting i saw it spelled out as flag so i searched for all the strings which contained things like this

So i wrote a simple command to show everyline which has the keyword SELECT using strings

-> strings web_access_ctf/web_access.log | grep -i "SELECT"



```
└─$ strings web_access_ctf/web_access.log | grep -i "SELECT"

192.168.0.92 - - [10/02/2024:01:32:28 +0000] "GET /search?id=1' OR SUBSTRING((SELECT f),1,1)='f' --  HTTP/2" 200 89
4 "-" "Safari/537.36"
192.168.0.198 - - [09/04/2024:02:29:55 +0000] "GET /search?id=1' OR SUBSTRING((SELECT l),1,1)='l' --  HTTP/2" 403 4
945 "-" "Chrome/91.0"
192.168.0.61 - - [27/06/2024:16:37:05 +0000] "GET /search?id=1' OR SUBSTRING((SELECT a),1,1)='a' --  HTTP/1.1" 500
1274 "http://test.com" "Safari/537.36"
192.168.0.88 - - [09/01/2024:23:01:49 +0000] "GET /search?id=1' OR SUBSTRING((SELECT g),1,1)='g' --  HTTP/2" 404 37
47 "http://test.com" "Mozilla/5.0"
192.168.0.172 - - [14/02/2024:02:19:58 +0000] "GET /search?id=1' OR SUBSTRING((SELECT {),1,1)='{' --  HTTP/1.1" 500
 4438 "http://test.com" "Safari/537.36"
192.168.0.97 - - [08/03/2024:12:02:23 +0000] "GET /search?id=1' OR SUBSTRING((SELECT s),1,1)='s' --  HTTP/2" 403 42
26 "http://test.com" "Chrome/91.0"
192.168.0.78 - - [19/04/2024:05:04:51 +0000] "POST /search?id=1' OR SUBSTRING((SELECT q),1,1)='q' --  HTTP/1.1" 403
 2959 "http://test.com" "Mozilla/5.0"
192.168.0.58 - - [05/04/2024:06:16:35 +0000] "GET /search?id=1' OR SUBSTRING((SELECT l),1,1)='l' --  HTTP/1.1" 200
1225 "http://test.com" "Mozilla/5.0"
192.168.0.34 - - [18/04/2024:04:31:29 +0000] "POST /search?id=1' OR SUBSTRING((SELECT _),1,1)='_' --  HTTP/2" 200 1
803 "http://test.com" "Chrome/91.0"
192.168.0.37 - - [15/12/2024:17:32:47 +0000] "GET /search?id=1' OR SUBSTRING((SELECT i),1,1)='i' --  HTTP/1.1" 500
3193 "http://example.com" "Mozilla/5.0"
192.168.0.244 - - [27/02/2024:19:30:23 +0000] "GET /search?id=1' OR SUBSTRING((SELECT n),1,1)='n' --  HTTP/2" 500 4
301 "-" "Safari/537.36"
192.168.0.141 - - [28/10/2024:03:57:13 +0000] "POST /search?id=1' OR SUBSTRING((SELECT j),1,1)='j' --  HTTP/2" 500
3596 "http://test.com" "Safari/537.36"
192.168.0.189 - - [14/11/2024:14:42:26 +0000] "POST /search?id=1' OR SUBSTRING((SELECT e),1,1)='e' --  HTTP/1.1" 20
0 340 "http://test.com" "Mozilla/5.0"
192.168.0.49 - - [17/08/2024:20:31:58 +0000] "GET /search?id=1' OR SUBSTRING((SELECT c),1,1)='c' --  HTTP/2" 200 79
2 "-" "Chrome/91.0"
192.168.0.48 - - [05/04/2024:16:22:20 +0000] "POST /search?id=1' OR SUBSTRING((SELECT t),1,1)='t' --  HTTP/2" 500 3
490 "-" "Safari/537.36"
192.168.0.229 - - [19/05/2024:14:18:57 +0000] "POST /search?id=1' OR SUBSTRING((SELECT i),1,1)='i' --  HTTP/1.1" 20
0 2023 "http://example.com" "Safari/537.36"
192.168.0.120 - - [14/05/2024:06:08:46 +0000] "GET /search?id=1' OR SUBSTRING((SELECT 0),1,1)='0' --  HTTP/1.1" 500
 3977 "-" "Mozilla/5.0"
192.168.0.73 - - [13/05/2024:16:56:30 +0000] "GET /search?id=1' OR SUBSTRING((SELECT n),1,1)='n' --  HTTP/2" 200 14
91 "-" "Chrome/91.0"
192.168.0.104 - - [08/01/2024:11:23:36 +0000] "GET /search?id=1' OR SUBSTRING((SELECT _),1,1)='_' --  HTTP/2" 404 2
56 "http://example.com" "Chrome/91.0"
192.168.0.16 - - [16/05/2024:09:58:15 +0000] "POST /search?id=1' OR SUBSTRING((SELECT a),1,1)='a' --  HTTP/1.1" 403
 1323 "http://test.com" "Chrome/91.0"
192.168.0.125 - - [17/01/2024:21:37:43 +0000] "POST /search?id=1' OR SUBSTRING((SELECT t),1,1)='t' --  HTTP/1.1" 40
4 3895 "-" "Safari/537.36"
192.168.0.179 - - [28/06/2024:07:43:49 +0000] "GET /search?id=1' OR SUBSTRING((SELECT t),1,1)='t' --  HTTP/2" 500 2
308 "http://test.com" "Mozilla/5.0"
192.168.0.172 - - [07/07/2024:10:06:35 +0000] "POST /search?id=1' OR SUBSTRING((SELECT a),1,1)='a' --  HTTP/1.1" 40
4 379 "http://example.com" "Mozilla/5.0"
192.168.0.65 - - [16/11/2024:17:46:12 +0000] "POST /search?id=1' OR SUBSTRING((SELECT c),1,1)='c' --  HTTP/1.1" 404
 1013 "http://example.com" "Safari/537.36"
192.168.0.139 - - [02/08/2024:00:50:50 +0000] "GET /search?id=1' OR SUBSTRING((SELECT k),1,1)='k' --  HTTP/1.1" 404
 4126 "http://test.com" "Safari/537.36"
```

And i got this

And we have our flag

flag-> ✅ **flag{sql_injection_attack}**