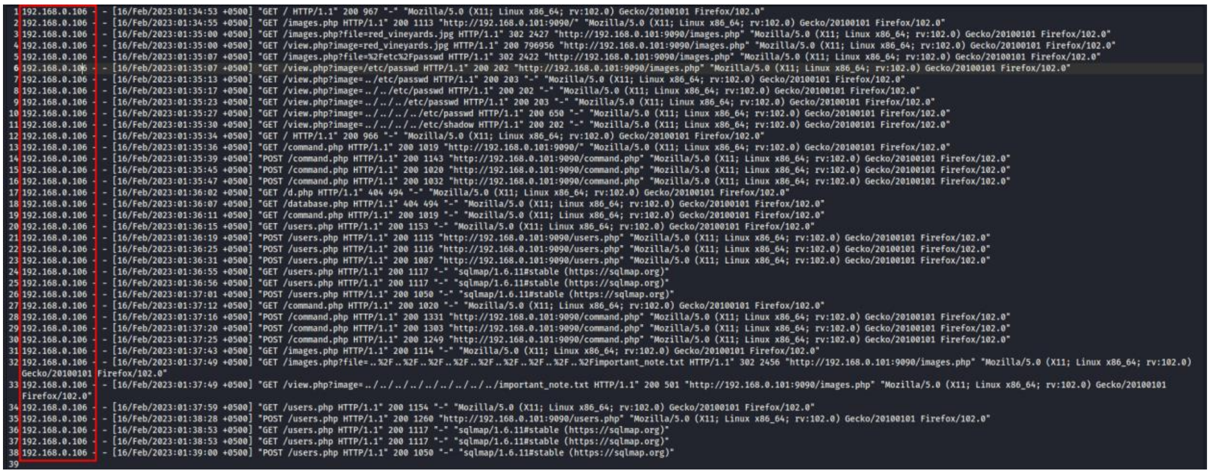
Digital Forensics-Lab#12

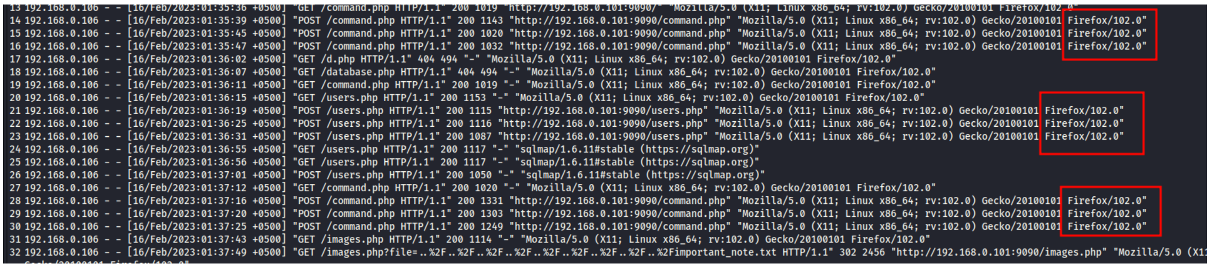
Ahmad Abdullah i22-1609

1.



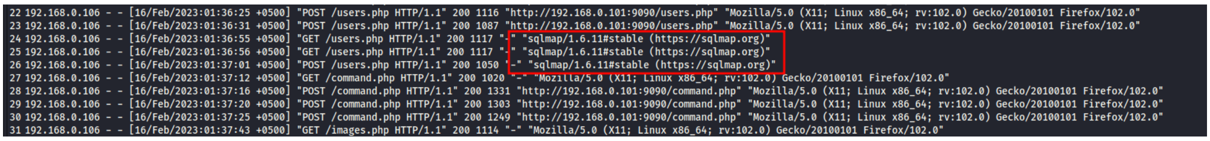
```
192.168.0.106 - - [16/Feb/2023:01:34:53 +0500] "GET / HTTP/1.1" 200 967 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:34:55 +0500] "GET /images.php HTTP/1.1" 200 1113 "http://192.168.0.101:9090/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:00 +0500] "GET /images.php?file=red_vineyards.jpg HTTP/1.1" 302 2427 "http://192.168.0.101:9090/images.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:00 +0500] "GET /view.php?image=red_vineyards.jpg HTTP/1.1" 200 796956 "http://192.168.0.101:9090/images.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:07 +0500] "GET /images.php?file=%2Fetc%2Fpasswd HTTP/1.1" 302 2422 "http://192.168.0.101:9090/images.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:07 +0500] "GET /view.php?image=/etc/passwd HTTP/1.1" 200 202 "http://192.168.0.101:9090/images.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:13 +0500] "GET /view.php?image=../etc/passwd HTTP/1.1" 200 203 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:17 +0500] "GET /view.php?image=../../etc/passwd HTTP/1.1" 200 202 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:23 +0500] "GET /view.php?image=../../../etc/passwd HTTP/1.1" 200 203 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:27 +0500] "GET /view.php?image=../../../../etc/passwd HTTP/1.1" 200 650 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:30 +0500] "GET /view.php?image=../../../../etc/shadow HTTP/1.1" 200 202 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:34 +0500] "GET / HTTP/1.1" 200 966 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:36 +0500] "GET /command.php HTTP/1.1" 200 1019 "http://192.168.0.101:9090/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:39 +0500] "POST /command.php HTTP/1.1" 200 1143 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:45 +0500] "POST /command.php HTTP/1.1" 200 1020 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:47 +0500] "POST /command.php HTTP/1.1" 200 1032 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:02 +0500] "GET /d.php HTTP/1.1" 404 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:07 +0500] "GET /database.php HTTP/1.1" 404 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:11 +0500] "GET /command.php HTTP/1.1" 200 1019 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:15 +0500] "GET /users.php HTTP/1.1" 200 1153 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:19 +0500] "POST /users.php HTTP/1.1" 200 1115 "http://192.168.0.101:9090/users.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:25 +0500] "POST /users.php HTTP/1.1" 200 1116 "http://192.168.0.101:9090/users.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:31 +0500] "POST /users.php HTTP/1.1" 200 1087 "http://192.168.0.101:9090/users.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:55 +0500] "GET /users.php HTTP/1.1" 200 1117 "-" "sqlmap/1.6.11#stable (https://sqlmap.org)"
192.168.0.106 - - [16/Feb/2023:01:36:56 +0500] "GET /users.php HTTP/1.1" 200 1117 "-" "sqlmap/1.6.11#stable (https://sqlmap.org)"
192.168.0.106 - - [16/Feb/2023:01:37:01 +0500] "POST /users.php HTTP/1.1" 200 1050 "-" "sqlmap/1.6.11#stable (https://sqlmap.org)"
192.168.0.106 - - [16/Feb/2023:01:37:12 +0500] "GET /command.php HTTP/1.1" 200 1020 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:16 +0500] "POST /command.php HTTP/1.1" 200 1331 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:20 +0500] "POST /command.php HTTP/1.1" 200 1303 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:25 +0500] "POST /command.php HTTP/1.1" 200 1249 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:43 +0500] "GET /images.php HTTP/1.1" 200 1114 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:49 +0500] "GET /images.php?file=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fimportant_note.txt HTTP/1.1" 302 2456 "http://192.168.0.101:9090/images.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:49 +0500] "GET /view.php?image=../../../../../../../../important_note.txt HTTP/1.1" 200 501 "http://192.168.0.101:9090/images.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:59 +0500] "GET /users.php HTTP/1.1" 200 1154 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:38:28 +0500] "POST /users.php HTTP/1.1" 200 1260 "http://192.168.0.101:9090/users.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:38:53 +0500] "GET /users.php HTTP/1.1" 200 1117 "-" "sqlmap/1.6.11#stable (https://sqlmap.org)"
192.168.0.106 - - [16/Feb/2023:01:38:53 +0500] "GET /users.php HTTP/1.1" 200 1117 "-" "sqlmap/1.6.11#stable (https://sqlmap.org)"
192.168.0.106 - - [16/Feb/2023:01:39:00 +0500] "POST /users.php HTTP/1.1" 200 1050 "-" "sqlmap/1.6.11#stable (https://sqlmap.org)"
```

2. Path Traversal
3. Firefox/102.0



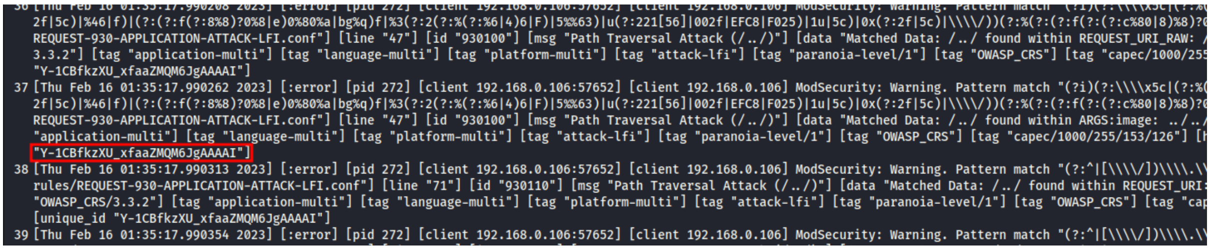
```
192.168.0.106 - - [16/Feb/2023:01:35:36 +0500] "GET /command.php HTTP/1.1" 200 1019 "http://192.168.0.101:9090/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:39 +0500] "POST /command.php HTTP/1.1" 200 1143 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:45 +0500] "POST /command.php HTTP/1.1" 200 1020 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:35:47 +0500] "POST /command.php HTTP/1.1" 200 1032 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:02 +0500] "GET /d.php HTTP/1.1" 404 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:07 +0500] "GET /database.php HTTP/1.1" 404 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:11 +0500] "GET /command.php HTTP/1.1" 200 1019 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:15 +0500] "GET /users.php HTTP/1.1" 200 1153 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:19 +0500] "POST /users.php HTTP/1.1" 200 1115 "http://192.168.0.101:9090/users.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:25 +0500] "POST /users.php HTTP/1.1" 200 1116 "http://192.168.0.101:9090/users.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:31 +0500] "POST /users.php HTTP/1.1" 200 1087 "http://192.168.0.101:9090/users.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:55 +0500] "GET /users.php HTTP/1.1" 200 1117 "-" "sqlmap/1.6.11#stable (https://sqlmap.org)"
192.168.0.106 - - [16/Feb/2023:01:36:56 +0500] "GET /users.php HTTP/1.1" 200 1117 "-" "sqlmap/1.6.11#stable (https://sqlmap.org)"
192.168.0.106 - - [16/Feb/2023:01:37:01 +0500] "POST /users.php HTTP/1.1" 200 1050 "-" "sqlmap/1.6.11#stable (https://sqlmap.org)"
192.168.0.106 - - [16/Feb/2023:01:37:12 +0500] "GET /command.php HTTP/1.1" 200 1020 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:16 +0500] "POST /command.php HTTP/1.1" 200 1331 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:20 +0500] "POST /command.php HTTP/1.1" 200 1303 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:25 +0500] "POST /command.php HTTP/1.1" 200 1249 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:43 +0500] "GET /images.php HTTP/1.1" 200 1114 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:49 +0500] "GET /images.php?file=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fimportant_note.txt HTTP/1.1" 302 2456 "http://192.168.0.101:9090/images.php" "Mozilla/5.0 (X1
```

4.

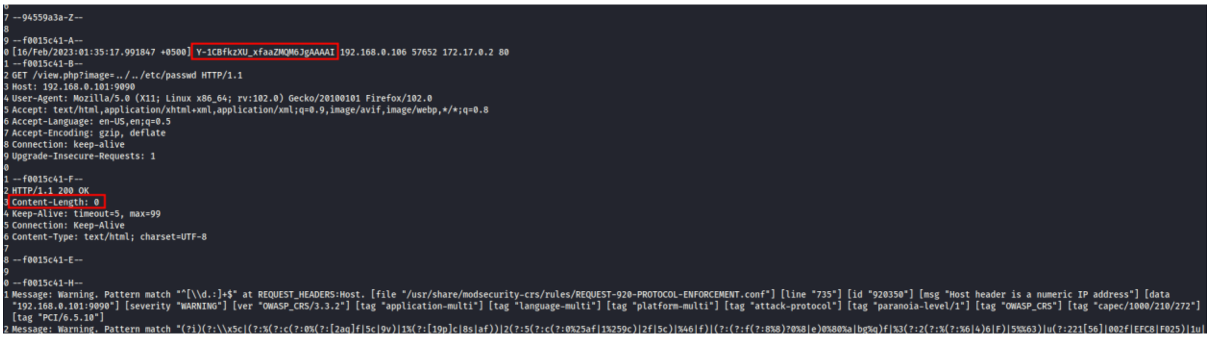


```
192.168.0.106 - - [16/Feb/2023:01:36:25 +0500] "POST /users.php HTTP/1.1" 200 1116 "http://192.168.0.101:9090/users.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:31 +0500] "POST /users.php HTTP/1.1" 200 1087 "http://192.168.0.101:9090/users.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:36:55 +0500] "GET /users.php HTTP/1.1" 200 1117 "-" "sqlmap/1.6.11#stable (https://sqlmap.org)"
192.168.0.106 - - [16/Feb/2023:01:36:56 +0500] "GET /users.php HTTP/1.1" 200 1117 "-" "sqlmap/1.6.11#stable (https://sqlmap.org)"
192.168.0.106 - - [16/Feb/2023:01:37:01 +0500] "POST /users.php HTTP/1.1" 200 1050 "-" "sqlmap/1.6.11#stable (https://sqlmap.org)"
192.168.0.106 - - [16/Feb/2023:01:37:12 +0500] "GET /command.php HTTP/1.1" 200 1020 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:16 +0500] "POST /command.php HTTP/1.1" 200 1331 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:20 +0500] "POST /command.php HTTP/1.1" 200 1303 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:25 +0500] "POST /command.php HTTP/1.1" 200 1249 "http://192.168.0.101:9090/command.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - - [16/Feb/2023:01:37:43 +0500] "GET /images.php HTTP/1.1" 200 1114 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
```

5. The attacker tried to access /passwd file. The server did respond with 200 OK reply but the content length was 0 which indicates that no data was shown.

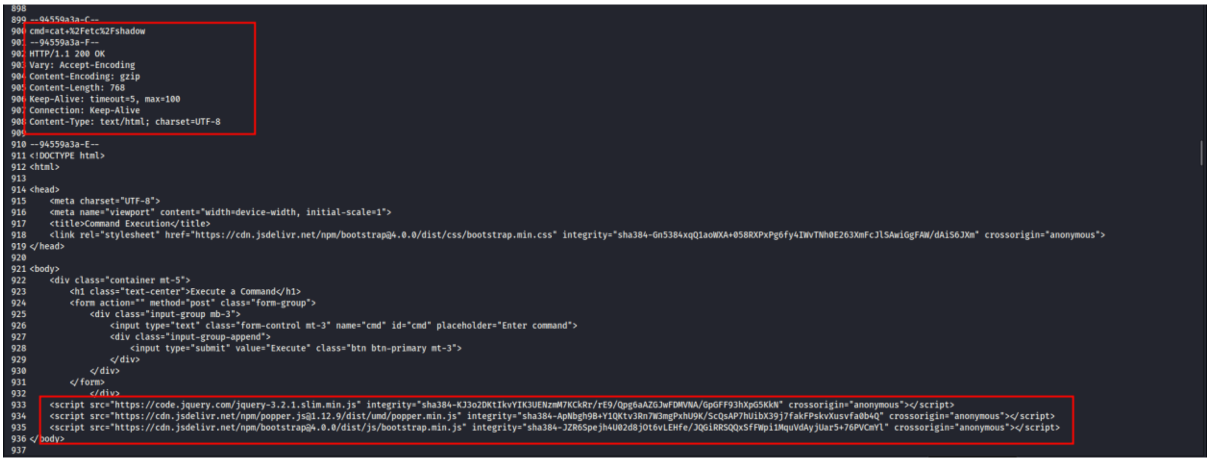


```
36 [Thu Feb 16 01:35:17.990208 2023] [:error] [pid 272] [client 192.168.0.106:57652] [client 192.168.0.106] ModSecurity: Warning. Pattern match "(?i)(?:\\\\x5c|(?:%
   2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|5c)|0x(?:2f|5c)|\\\\/))(?:%(?:(?:f(?:(?:c%80|8)%8)?0
   REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "47"] [id "930100"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: /../ found within REQUEST_URI_RAW: /
   3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-lfi"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/255
   "Y-1CBfkzXU_xfaaZMQM6JgAAAAI"]
37 [Thu Feb 16 01:35:17.990262 2023] [:error] [pid 272] [client 192.168.0.106:57652] [client 192.168.0.106] ModSecurity: Warning. Pattern match "(?i)(?:\\\\x5c|(?:%(
   2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|5c)|0x(?:2f|5c)|\\\\/))(?:%(?:(?:f(?:(?:c%80|8)%8)?0
   REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "47"] [id "930100"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: /../ found within ARGS:image: ../../
   "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-lfi"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/255/153/126"] [h
   "Y-1CBfkzXU_xfaaZMQM6JgAAAAI"]
38 [Thu Feb 16 01:35:17.990313 2023] [:error] [pid 272] [client 192.168.0.106:57652] [client 192.168.0.106] ModSecurity: Warning. Pattern match "(?:^|[\\\\/])\\\\.\\
   rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "71"] [id "930110"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: /../ found within REQUEST_URI:
   "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-lfi"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "cap
   [unique_id "Y-1CBfkzXU_xfaaZMQM6JgAAAAI"]
39 [Thu Feb 16 01:35:17.990354 2023] [:error] [pid 272] [client 192.168.0.106:57652] [client 192.168.0.106] ModSecurity: Warning. Pattern match "(?:^|[\\\\/])\\\\.\\
```



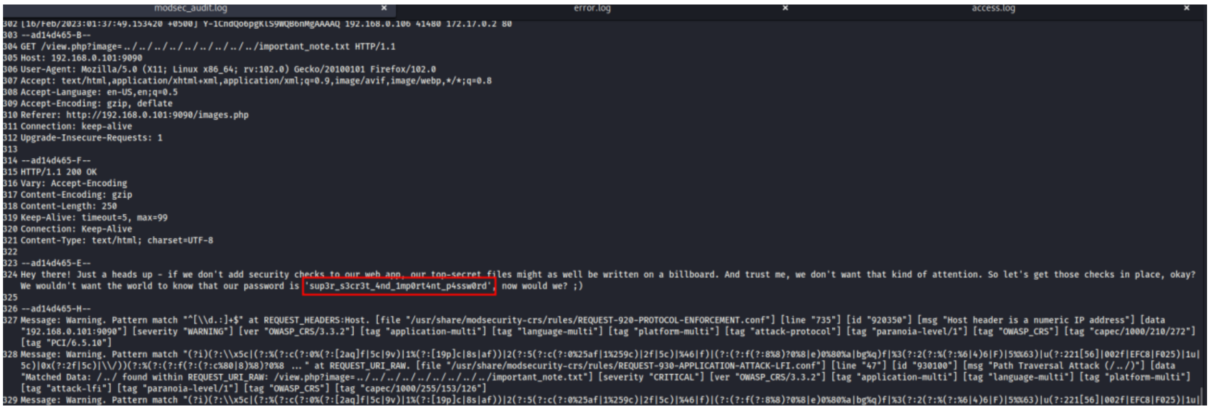
```
--94559a3a-Z--

--f0015c41-A--
[16/Feb/2023:01:35:17.991847 +0500] Y-1CBfkzXU_xfaaZMQM6JgAAAAI 192.168.0.106 57652 172.17.0.2 80
--f0015c41-B--
GET /view.php?image=../../etc/passwd HTTP/1.1
Host: 192.168.0.101:9090
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: keep-alive
Upgrade-Insecure-Requests: 1

--f0015c41-F--
HTTP/1.1 200 OK
Content-Length: 0
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

--f0015c41-E--

--f0015c41-H--
Message: Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host. [file "/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "735"] [id "920350"] [msg "Host header is a numeric IP address"] [data
 "192.168.0.101:9090"] [severity "WARNING"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/210/272"]
 [tag "PCI/6.5.10"]
Message: Warning. Pattern match "(?i)(?:\\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|2(?:5(?:c(?:0%25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|
```

6. The attacker kept trying to access data using SQL map in which they did succeed and got some confidential user data.



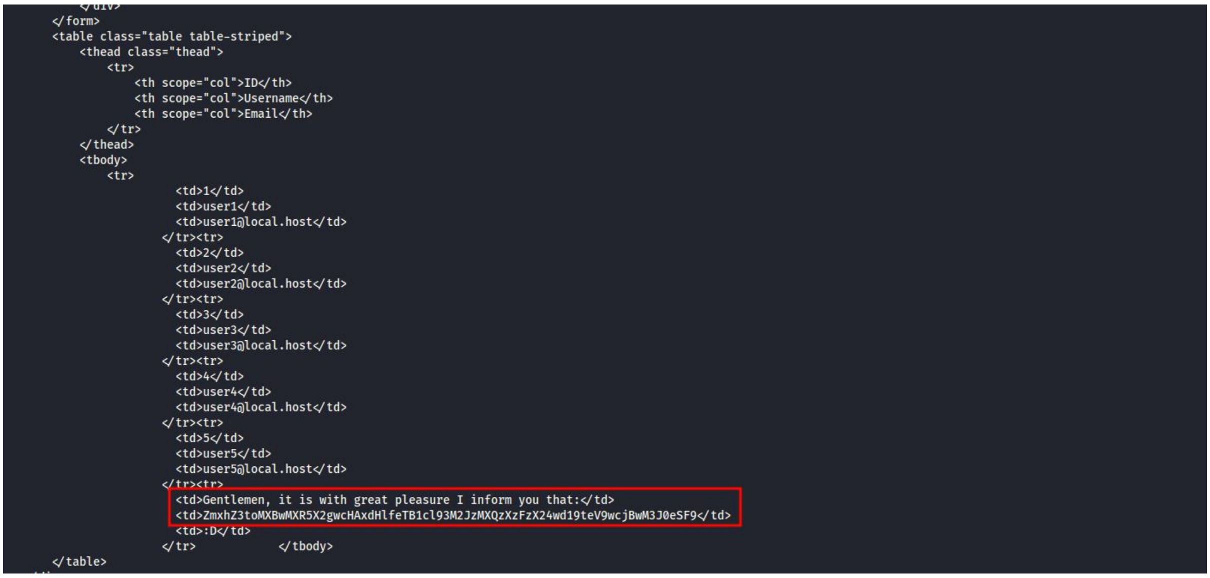
```

--94559a3a-C--
cmd=cat+%2Fetc%2Fshadow
--94559a3a-F--
HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 768
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

--94559a3a-E--
<!DOCTYPE html>
<html>

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Command Execution</title>
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@4.0.0/dist/css/bootstrap.min.css" integrity="sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm" crossorigin="anonymous">
</head>

<body>
    <div class="container mt-5">
        <h1 class="text-center">Execute a Command</h1>
        <form action="" method="post" class="form-group">
            <div class="input-group mb-3">
                <input type="text" class="form-control mt-3" name="cmd" id="cmd" placeholder="Enter command">
                <div class="input-group-append">
                    <input type="submit" value="Execute" class="btn btn-primary mt-3">
                </div>
            </div>
        </form>
            </div>
    <script src="https://code.jquery.com/jquery-3.2.1.slim.min.js" integrity="sha384-KJ3o2DKtIkvYIK3UENzmM7KCkRr/rE9/Qpg6aAZGJwFDMVNA/GpGFF93hXpG5KkN" crossorigin="anonymous"></script>
    <script src="https://cdn.jsdelivr.net/npm/popper.js@1.12.9/dist/umd/popper.min.js" integrity="sha384-ApNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hUibX39j7fakFPskvXusvfa0b4Q" crossorigin="anonymous"></script>
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@4.0.0/dist/js/bootstrap.min.js" integrity="sha384-JZR6Spejh4U02d8jOt6vLEHfe/JQGiRRSQQxSfFWpi1MquVdAyjUar5+76PVCmYl" crossorigin="anonymous"></script>
</body>

```

7.



```
[16/Feb/2023:01:37:49.153420 +0500] Y-1CndQo6pgKtS9WQB6nMgAAAAQ 192.168.0.106 41480 172.17.0.2 80
--ad14d465-B--
GET /view.php?image=../../../../../../../../../important_note.txt HTTP/1.1
Host: 192.168.0.101:9090
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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://192.168.0.101:9090/images.php
Connection: keep-alive
Upgrade-Insecure-Requests: 1

--ad14d465-F--
HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 250
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

--ad14d465-E--
Hey there! Just a heads up - if we don't add security checks to our web app, our top-secret files might as well be written on a billboard. And trust me, we don't want that kind of attention. So let's get those checks in place, okay?
 We wouldn't want the world to know that our password is 'sup3r_s3cr3t_4nd_1mp0rt4nt_p4ssw0rd', now would we? ;)

--ad14d465-H--
Message: Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host. [file "/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "735"] [id "920350"] [msg "Host header is a numeric IP address"] [data
 "192.168.0.101:9090"] [severity "WARNING"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/210/272"]
 [tag "PCI/6.5.10"]
Message: Warning. Pattern match "(?i)(?:\\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|2(?:5(?:c(?:0%25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|
 5c)|0x(?:2f|5c)|\\/))(?:%(?:(?:f(?:(?:c%80|8)%8)?0%8 ..." at REQUEST_URI_RAW. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "47"] [id "930100"] [msg "Path Traversal Attack (/../)"] [data
 "Matched Data: /../ found within REQUEST_URI_RAW: /view.php?image=../../../../../../../../../important_note.txt"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"]
 [tag "attack-lfi"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/255/153/126"]
Message: Warning. Pattern match "(?i)(?:\\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|2(?:5(?:c(?:0%25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|
```

8. flag{h1pp1ty_h0pp1ty_y0ur_w3bs1t3_1s_n0w_my_pr0p3rty!}



```
    </div>
</form>
<table class="table table-striped">
    <thead class="thead">
        <tr>
            <th scope="col">ID</th>
            <th scope="col">Username</th>
            <th scope="col">Email</th>
        </tr>
    </thead>
    <tbody>
        <tr>
                  <td>1</td>
                  <td>user1</td>
                  <td>user1@local.host</td>
                </tr><tr>
                  <td>2</td>
                  <td>user2</td>
                  <td>user2@local.host</td>
                </tr><tr>
                  <td>3</td>
                  <td>user3</td>
                  <td>user3@local.host</td>
                </tr><tr>
                  <td>4</td>
                  <td>user4</td>
                  <td>user4@local.host</td>
                </tr><tr>
                  <td>5</td>
                  <td>user5</td>
                  <td>user5@local.host</td>
                </tr><tr>
                  <td>Gentlemen, it is with great pleasure I inform you that:</td>
                  <td>ZmxhZ3toMXBwMXR5X2gwcHAxdHlfeTB1cl93M2JzMXQzXzFzX24wd19teV9wcjBwM3J0eSF9</td>
                  <td>:D</td>
                </tr>            </tbody>
</table>
```

9. The indicators that confirmed that an attack had taken place were Remote Code Execution, SQL injection etc. The key takeaway from this is that we used to refine our code to better handle the requests for all the known vulnerabilities.
10. SQL injection, Path Traversal, Remote Code Execution etc.