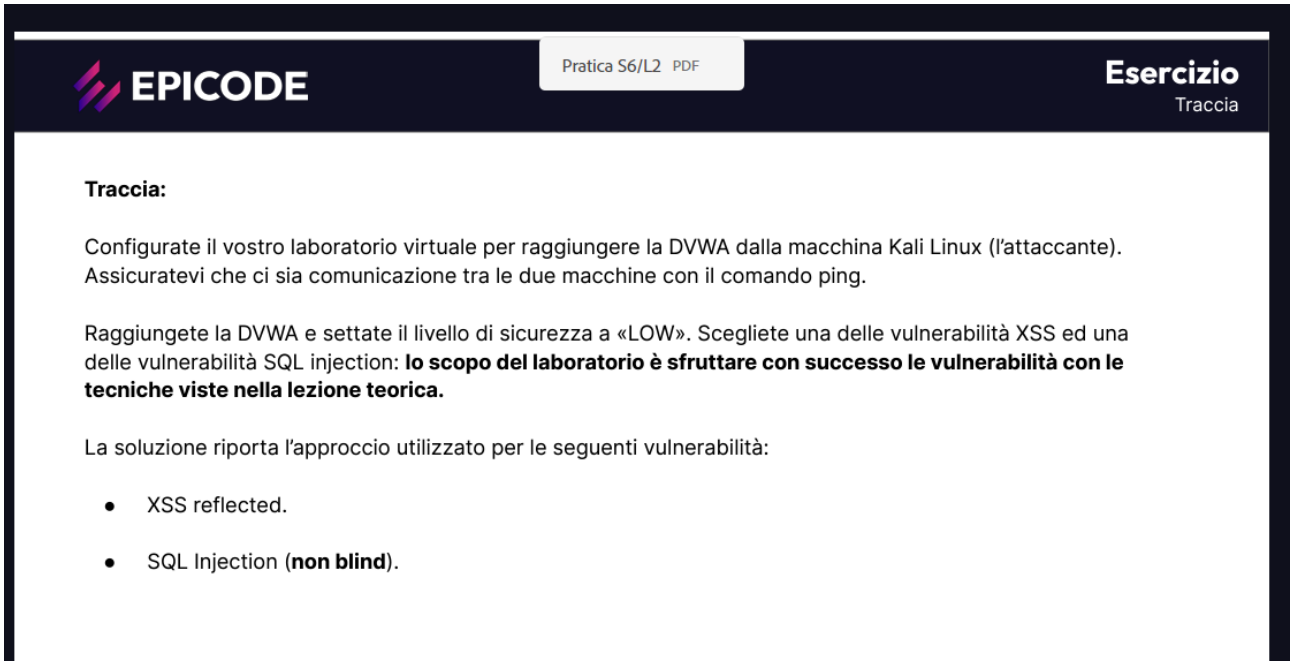
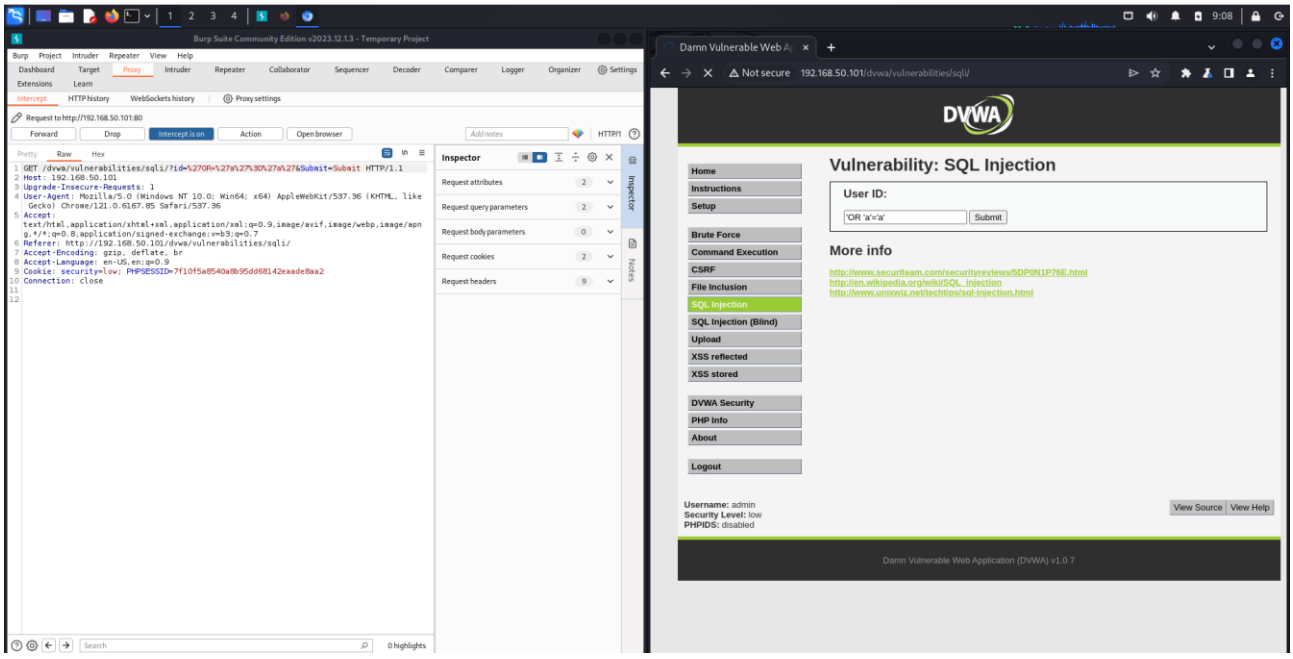
“RISOLUZIONE ESERCIZIO S6L2”

TRACCIA



SOLUZIONE PER SQL INJECTION



ABBIAMO INSERITO IL COMANDO

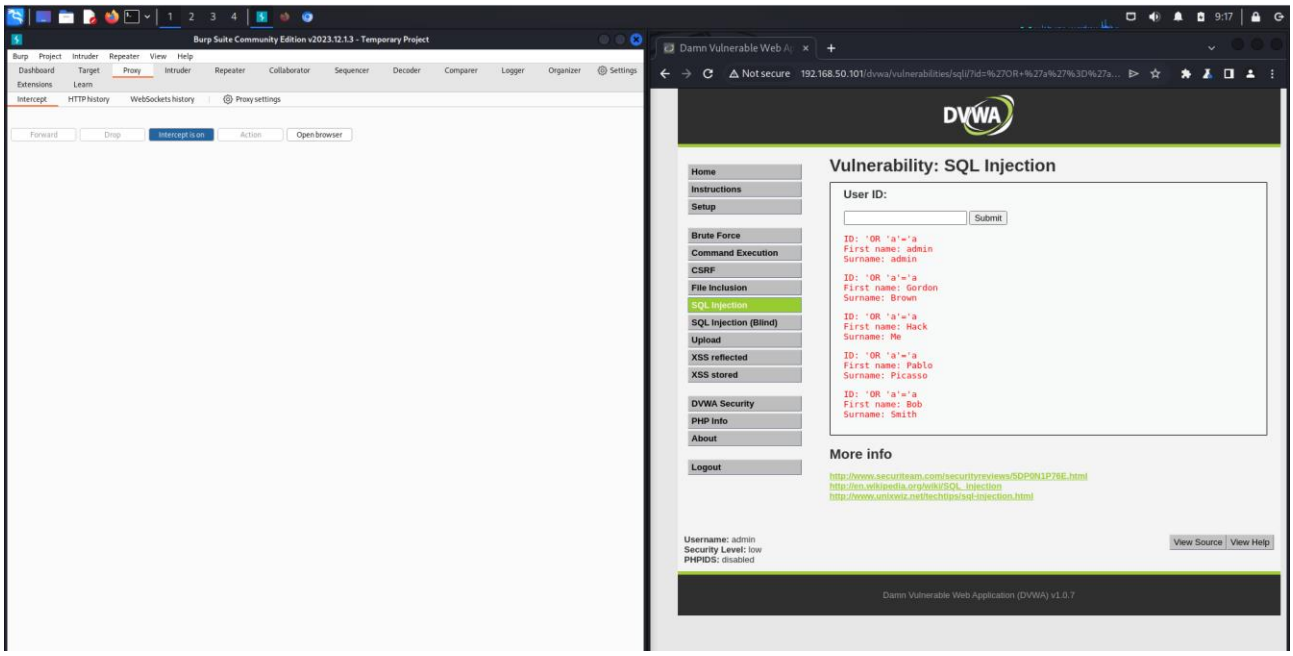
OR ‘a’ = ‘a’

CHE CI FA ACCEDERE ALLA TABELLA PRESENTE SULLA DVWA IN MODO DA VISUALIZZARE I RELATIVI CAMPI :

ID

FIRST NAME

SURNAME



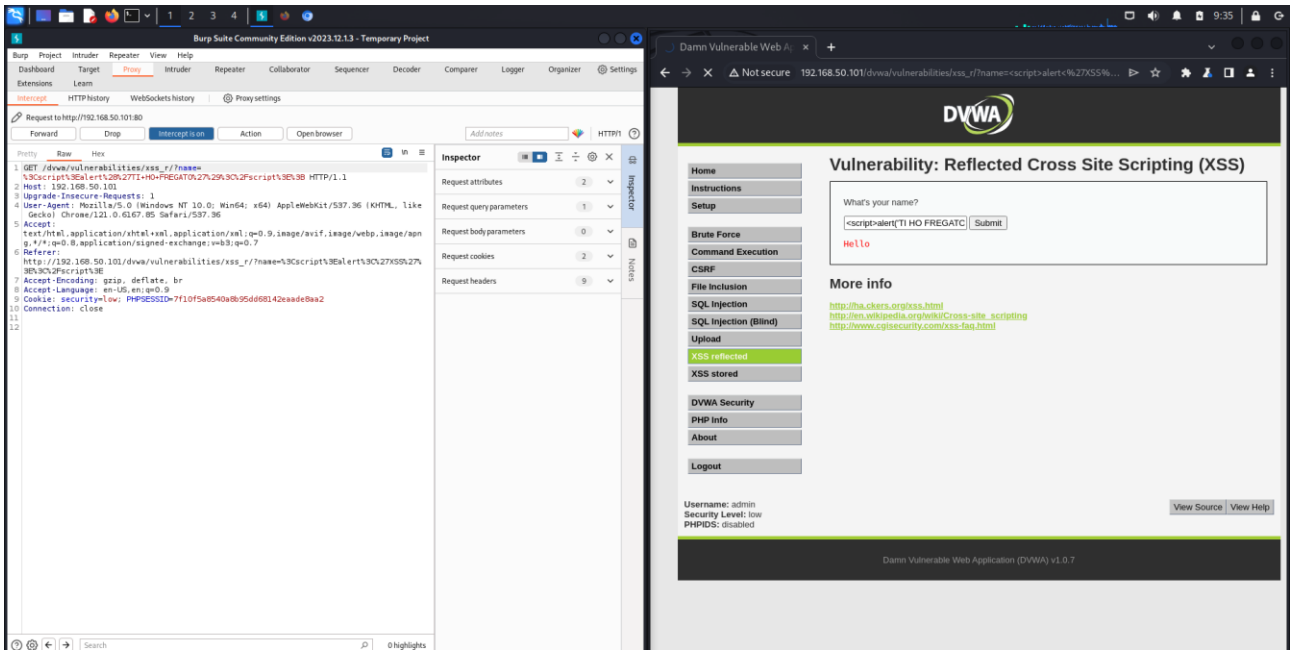
PER PREVENIRE QUESTO ATTACCO POTREMMO INSERIRE UN COMANDO PER FARE IN MODO CHE I CARATTERI SPECIALI VENGANO LETTI COME CARATTERI DI TESTO

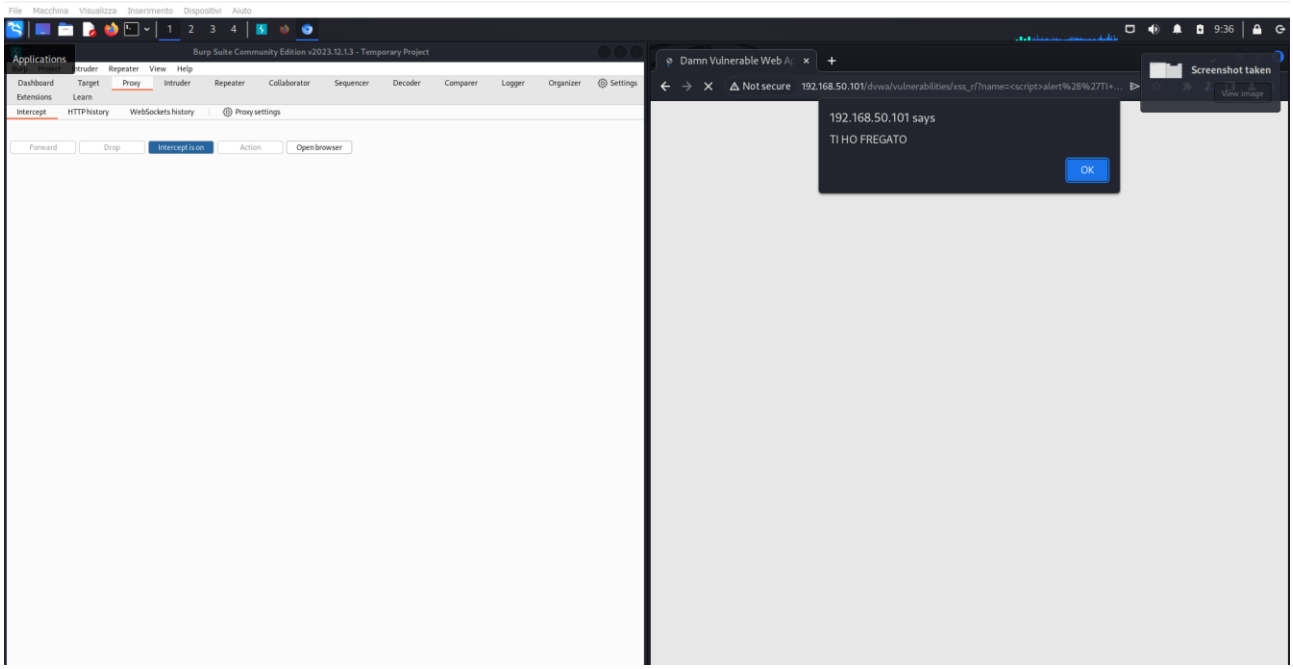
ES.

```
$id = $_GET['id'];
$id = stripslashes($id);
$id = mysql_real_escape_string($id);
```

O AGGIUNGENDO DEI TOKEN DI SESSIONE OLTRE AI COOKIE

“SOLUZIONE CON XSS REFLECTED”





IN QUESTO CASO ABBIAMO INFETTATO IL PAYLOAD FACENDOGLI APPARIRE UNA RIGA DI TESTO

In questo caso abbiamo preso username e password inerente ai data base