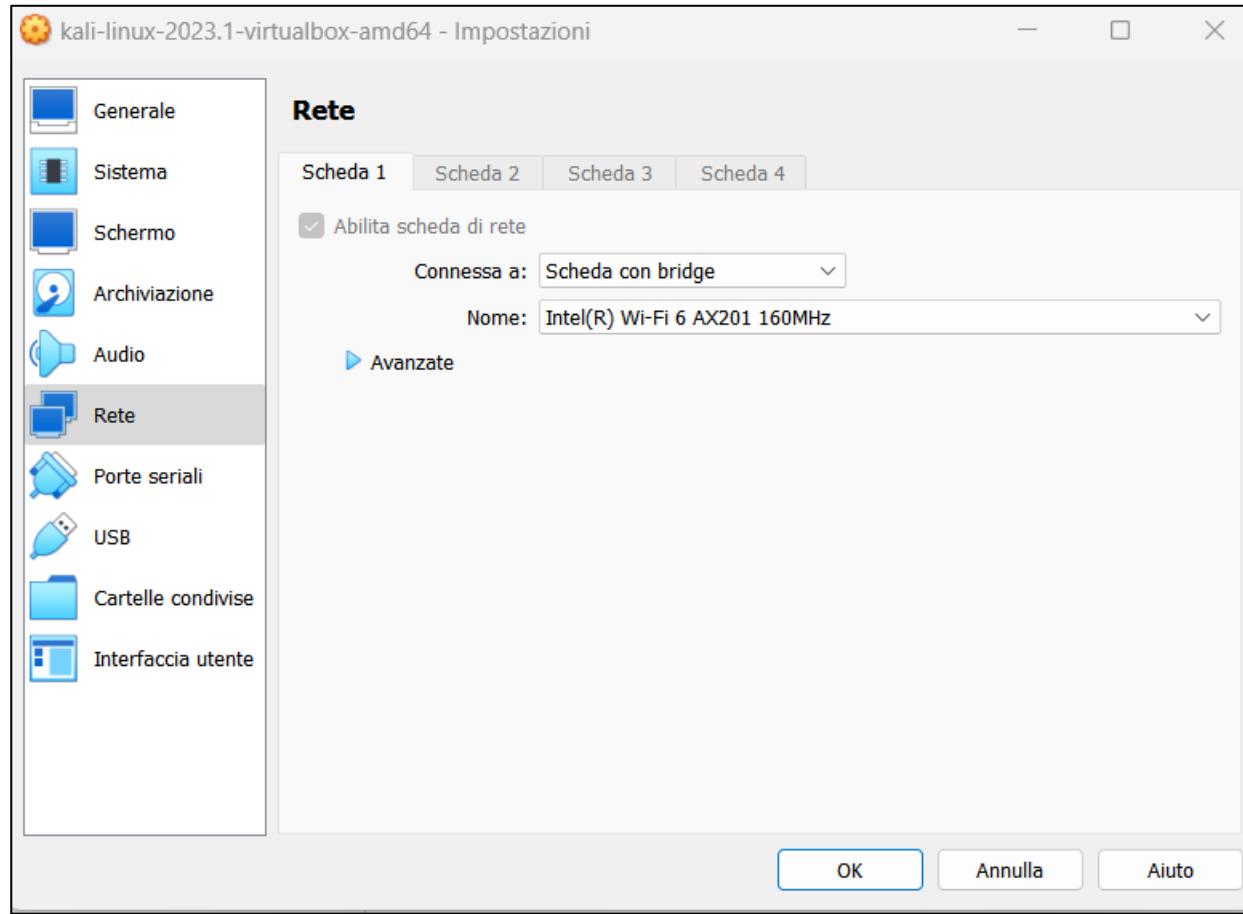


Configurazione VM per la navigazione su WEB

Oracle VirtualBox



Linux /etc/network/interfaces

```
GNU nano /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.10
netmask 255.255.255.0
gateway 192.168.1.254

#address 192.168.32.100/24
#gateway 192.168.32.1
#iface eth0 inet dhcp
```

Home

Instructions

Setup / Run

Brute Force

Commands

Congurazione utente su MariaDB

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo mysql -u root -p
[sudo] password for kali:
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 56
Server version: 10.11.2-MariaDB-1 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SHOW GRANTS for 'kali'@'127.0.0.1' ;
+-----+-----+
| Grants for kali@127.0.0.1 |
+-----+-----+
| GRANT USAGE ON *.* TO `kali`@`127.0.0.1` IDENTIFIED BY PASSWORD '*D64F6611CF18EA567ED1E8E74F2243AC1EDF54C4' |
| GRANT ALL PRIVILEGES ON `dvwa`.* TO `kali`@`127.0.0.1` |
+-----+-----+
2 rows in set (0.000 sec)

MariaDB [(none)]> exit
Bye
(kali㉿kali)-[~]
$
```

Configurazione Apache2

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ service apache2 start

(kali㉿kali)-[~]
$ cd /etc/php/8.2/apache2

(kali㉿kali)-[/etc/php/8.2/apache2]
$ nano php.ini
File System
```

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On
```

Burpsuite

```
(kali㉿kali)-[~]
$ service apache2 start
```

ObjectIntruderRepeaterWindowHelp


rdTargetProxyIntruderRepeaterSequencerDecoder

HTTP historyWebSockets historyProxy settings

ardDropIntercept is onActionOpen browser

Login :: Damn Vulnerable x +

127.0.0.1/DVWA/login.php



Username

admin

Password

Login

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLoggerExtensionsLearn

InterceptHTTP historyWebSockets historyProxy settings

Request to http://127.0.0.1:80

ForwardDropIntercept is onActionOpen browser

PrettyRawHex

1 POST /DVWA/login.php HTTP/1.1

2 Host: 127.0.0.1

3 Content-Length: 88

4 Cache-Control: max-age=0

5 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"

6 sec-ch-ua-mobile: ?0

7 sec-ch-ua-platform: "Linux"

8 Upgrade-Insecure-Requests: 1

9 Origin: http://127.0.0.1

10 Content-Type: application/x-www-form-urlencoded

11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36

12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8

13 Sec-Fetch-Site: same-origin

14 Sec-Fetch-Mode: navigate

15 Sec-Fetch-User: ?1

16 Sec-Fetch-Dest: document

17 Referer: http://127.0.0.1/DVWA/login.php

18 Accept-Encoding: gzip, deflate

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

20 Cookie: PHPSESSID=ki6dknlu6rkqki157pajphutab; security=impossible

21 Connection: close

22

23 username=ciao&password=bella&Login=Login&user_token=c4936d5d855f4d92ceb73ad0d9376e83

Scan

Scan selected insertion point

Send to IntruderCtrl+I

Send to RepeaterCtrl+R

Send to Sequencer

Send to Comparer

Send to Decoder

Insert Collaborator payload

Request in browser>

Engagement tools [Pro version only]>

Change request method

Change body encoding

Copy URL

SendCancel<>>

Request

Raw

Hex

1

GET /DVWA/login.php HTTP/1.1

2

Host: 127.0.0.1

3

Cache-Control: max-age=0

4

sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"

5

sec-ch-ua-mobile: ?0

6

sec-ch-ua-platform: "Linux"

7

Upgrade-Insecure-Requests: 1

8

Origin: http://127.0.0.1

9

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36

10

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

11

Sec-Fetch-Site: same-origin

12

Sec-Fetch-Mode: navigate

13

Sec-Fetch-User: ?1

14

Sec-Fetch-Dest: document

15

Referer: http://127.0.0.1/DVWA/login.php

16

Accept-Encoding: gzip, deflate

17

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

18

Cookie: PHPSESSID=ki6dknlu6rkqki157pajphutab; security=impossible

19

Connection: close

20

21

Response

Pretty

Raw

Hex

Render

47

48

49

<label for="pass">
Password
</label>
<input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="password">

50

51

52

53

<p class="submit">
<input type="submit" value="Login" name="Login">
</p>

54

55

</fieldset>

56

57

<input type='hidden' name='user_token' value='651f50af3ab72426bdc42a329a6e6cc5' />

58

59

</form>

60

61

62

63

<div class="message">
Login failed
</div>

64

65

66

67

68

69