

Esercizio S3L2

MIRKA FEBBO

Introduction

Traccia: Nella lezione pratica di oggi abbiamo visto come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

```
root@kali: /etc/php/8.4/apache2

Actions Edit View Help

kali@kali)-[~]
sudo su
o] password for kali:
root@kali)-[/home/kali]
cd /var/www/html

root@kali)-[/var/www/html]
git clone https://github.com/digininja/DVWA
ing into 'DVWA' ...
te: Enumerating objects: 5373, done.
te: Total 5373 (delta 0), reused 0 (delta 0), pack-reused 5373 (f
iving objects: 100% (5373/5373), 2.57 MiB | 6.64 MiB/s, done.
lving deltas: 100% (2673/2673), done.

root@kali)-[/var/www/html]
chown -R www-data:www-data DVWA/

root@kali)-[/var/www/html]
cd DVWA/config

root@kali)-[/var/www/html/DVWA/config]
cp config.inc.php.dist config.inc.php

root@kali)-[/var/www/html/DVWA/config]
nano config.inc.php

root@kali)-[/var/www/html/DVWA/config]
cd
```

Seguendo le slide, abbiamo installato DVWA dal terminale di Kali, così come l'apache2. Nel codice che ti apre bisogna ricordarsi di modificare user e password, oltre che il livello di sicurezza in low

```
root@kali: /etc/php/8.4/apache2

File Actions Edit View Help

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

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

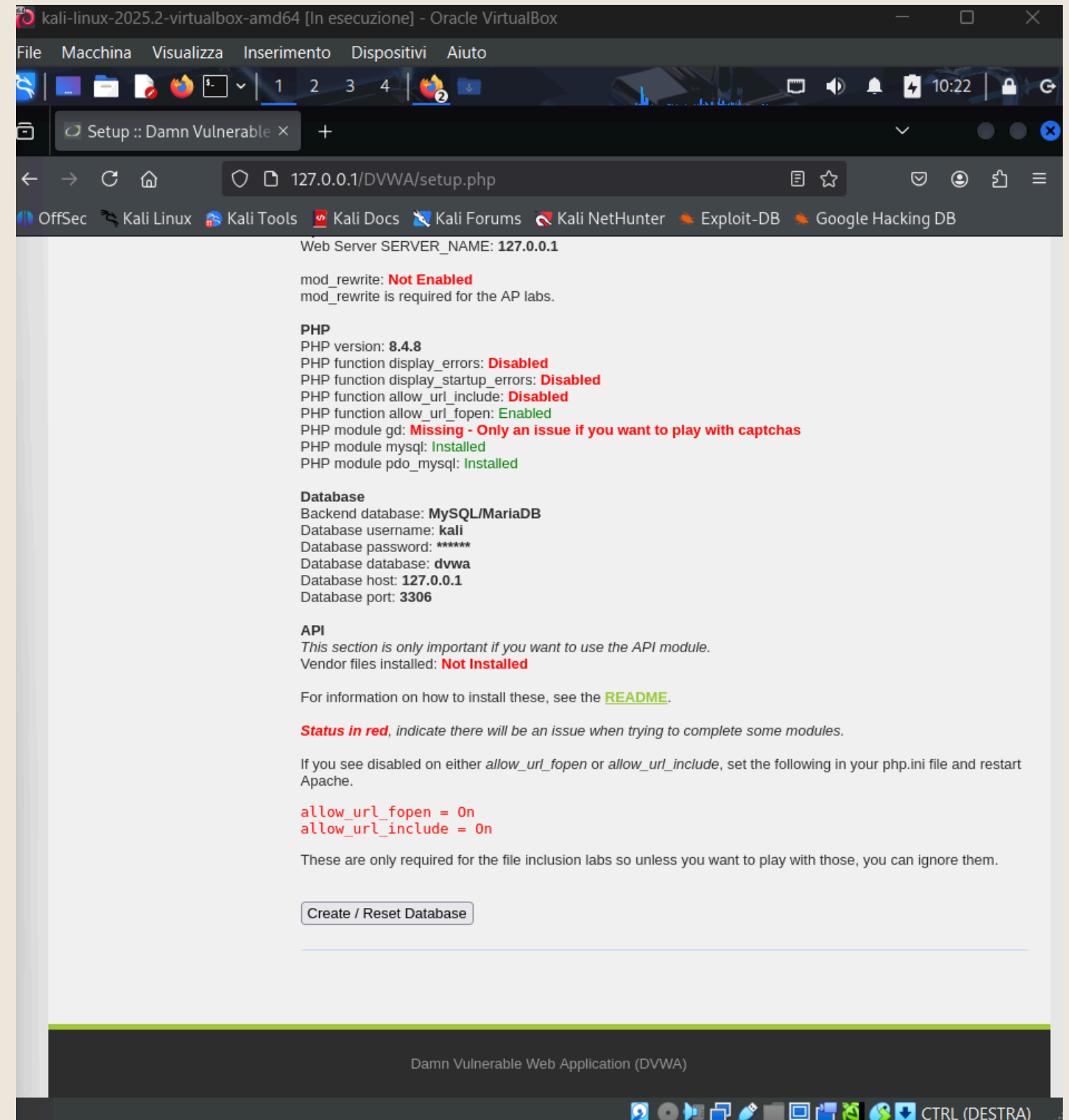
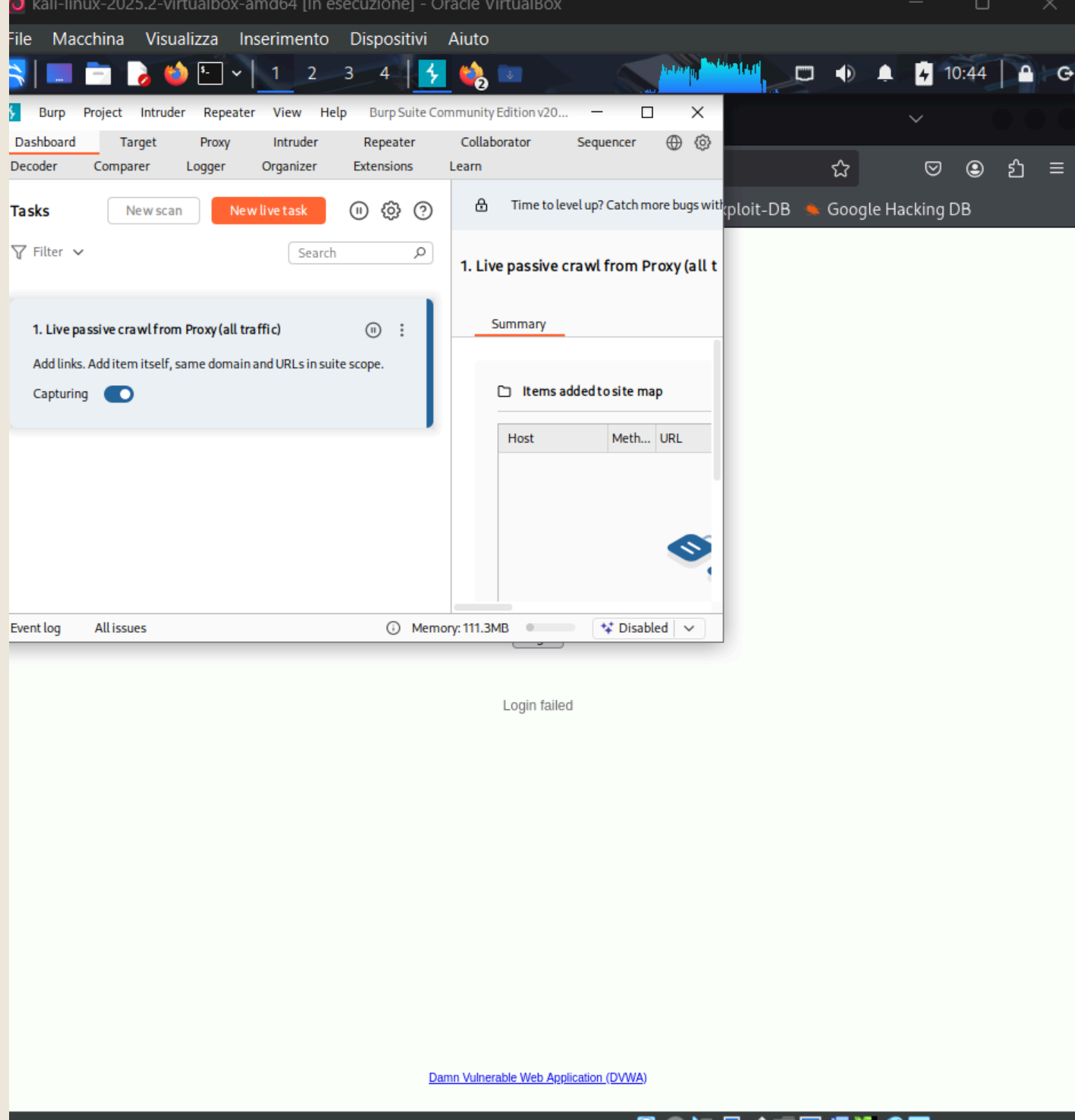
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.008 sec)

MariaDB [(none)]> grant all privileges on dvwa.*to 'kali'@127.0.0.1' o
ed by 'kali'
      '> grant all privileges on dvwa.*to 'kali'@127.0.0.1' odentified by
';
ERROR 1064 (42000): You have an error in your SQL syntax; check the man
at corresponds to your MariaDB server version for the right syntax to
r '' odentified by 'kali'
grant all privileges on dvwa.*to 'kali'@127.0.0.1' ode ... ' at line 1
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1'
fied by 'kali' ;
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> exit
Bye

(root@kali)-[~]
# service apache2 start

(root@kali)-[~]
```



Una volta eseguito le installazioni, passiamo sul browser e mettiamo nella barra di ricerca “127.0.0.1/DVWA/setup.php” e clicchiamo su creat, successivamente avremo la pagina di login, ora apriamo burb suite cliccando su send e successivamente su follow...

A questo punto, non ci resta che eseguire il login e avremo il collegamento per cui tutto ciò che eseguiamo sul browser lo vedremo, potendolo anche modificare da burbsuite.

The image shows a Kali Linux virtual machine running Burp Suite and a web browser. The browser window displays the DVWA (Damn Vulnerable Web Application) login page. The username field is filled with 'admin' and the password field is filled with '*****'. The 'Login' button is visible. The Burp Suite interface is open, showing the 'Repeater' tab. The 'Request' pane displays the HTTP request details, including the 'Host' (127.0.0.1) and various headers. The 'Response' pane shows the HTML response, indicating a 'Login failed' message. The status bar at the bottom of Burp Suite shows 'Done' and 'Event log (1)'.

Request Details:

```
1 SET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
7 Accept-Language: en-US,en;q=0.9
8 Origin: http://127.0.0.1
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
11 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
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
```

Response Details:

```
61 <br />
62
63 <div class="message">
64   Login failed
65 </div>
66 <br />
67 <br />
68 <br />
69 <br />
70 <br />
71 <br />
72 <br />
73 <br />
74 </div>
75 <!--div id="content">-->
```