

Consegna S3-L3

Utilizzo di Burpsuite

Traccia

- Nella lezione pratica di oggi vedremo come configurare una DVWA - ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test sia durante la build week 1 che durante lo sviluppo del modulo 2, dove vedremo da vicino le tecniche per sfruttare le vulnerabilità nella fase di exploit.

Configurazione

Seguendo i passaggi dell'esercizio sono arrivato a configurare sia il database MySQL che il Web Server Apache. In questo screenshot l'ultimo passaggio dove metto su 'On' la stringa «allow_url_include»

```
; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
; https://php.net/upload-tmp-dir
upload_tmp_dir =

; Maximum allowed size for uploaded files.
; https://php.net/upload-max-filesize
upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

;;;;;;;;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;;;;;;;;

; 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

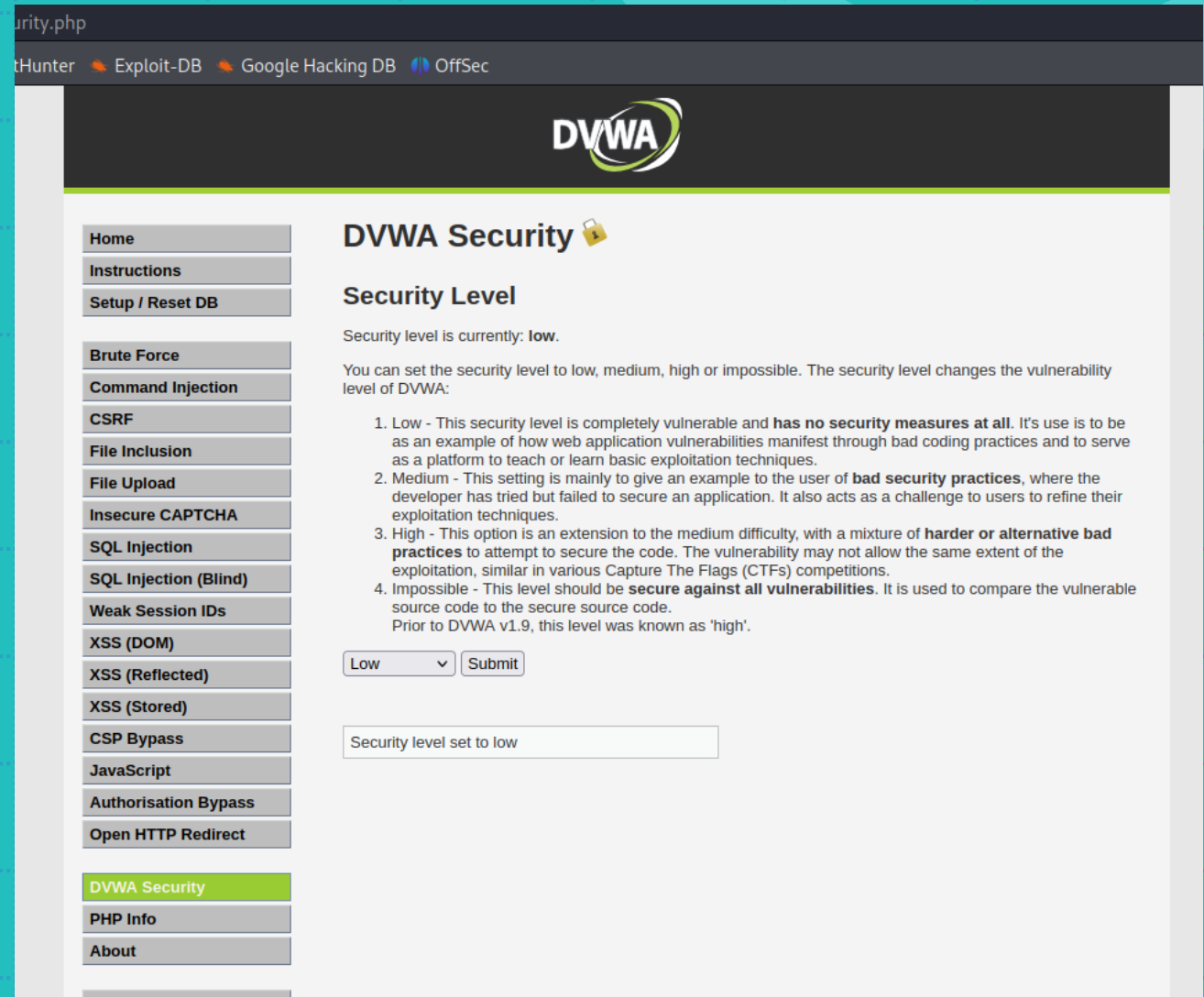
; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; https://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; https://php.net/user-agent
user_agent="PHP"

; Default timeout for socket based streams (seconds)
; https://php.net/default-socket-timeout
default_socket_timeout = 60
```

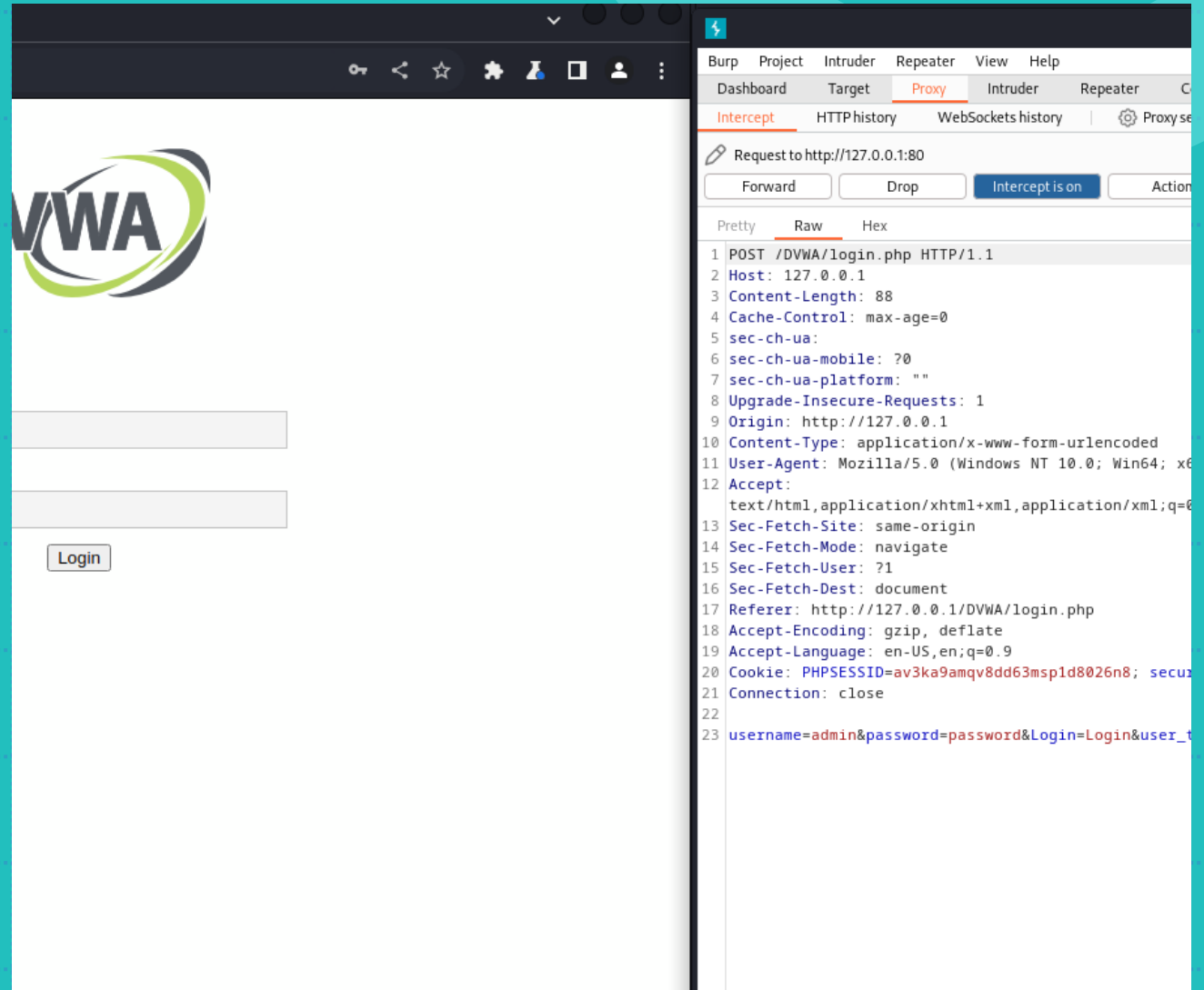
Diminuire il livello di sicurezza

Inserendo
127.0.0.1/DVWA/setup.php sulla
barra degli indirizzi del mio browser
ho fatto l'accesso alla pagina DVWA
Security ed ho impostato il livello di
sicurezza a Low



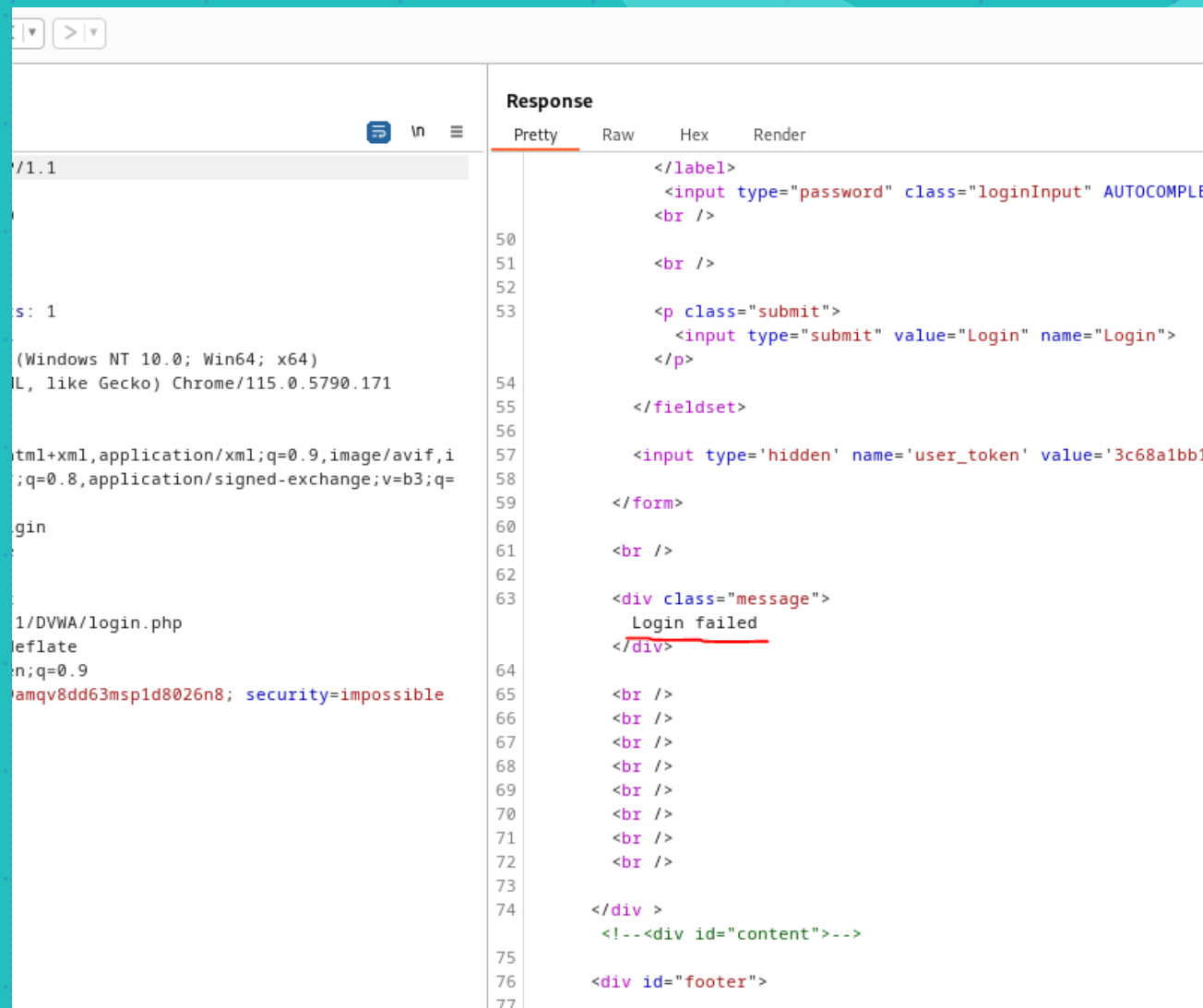
Intercettazione della richiesta con Burp

Avviando Burp, abbiamo potuto intercettare una richiesta di login ad un sito tramite browser. Possiamo ottenere varie informazioni tra le quali username e password di login



Errore di accesso

Se andiamo a modificare le credenziali di login e tentiamo un accesso, apparirà l'informazione che il Login è fallito



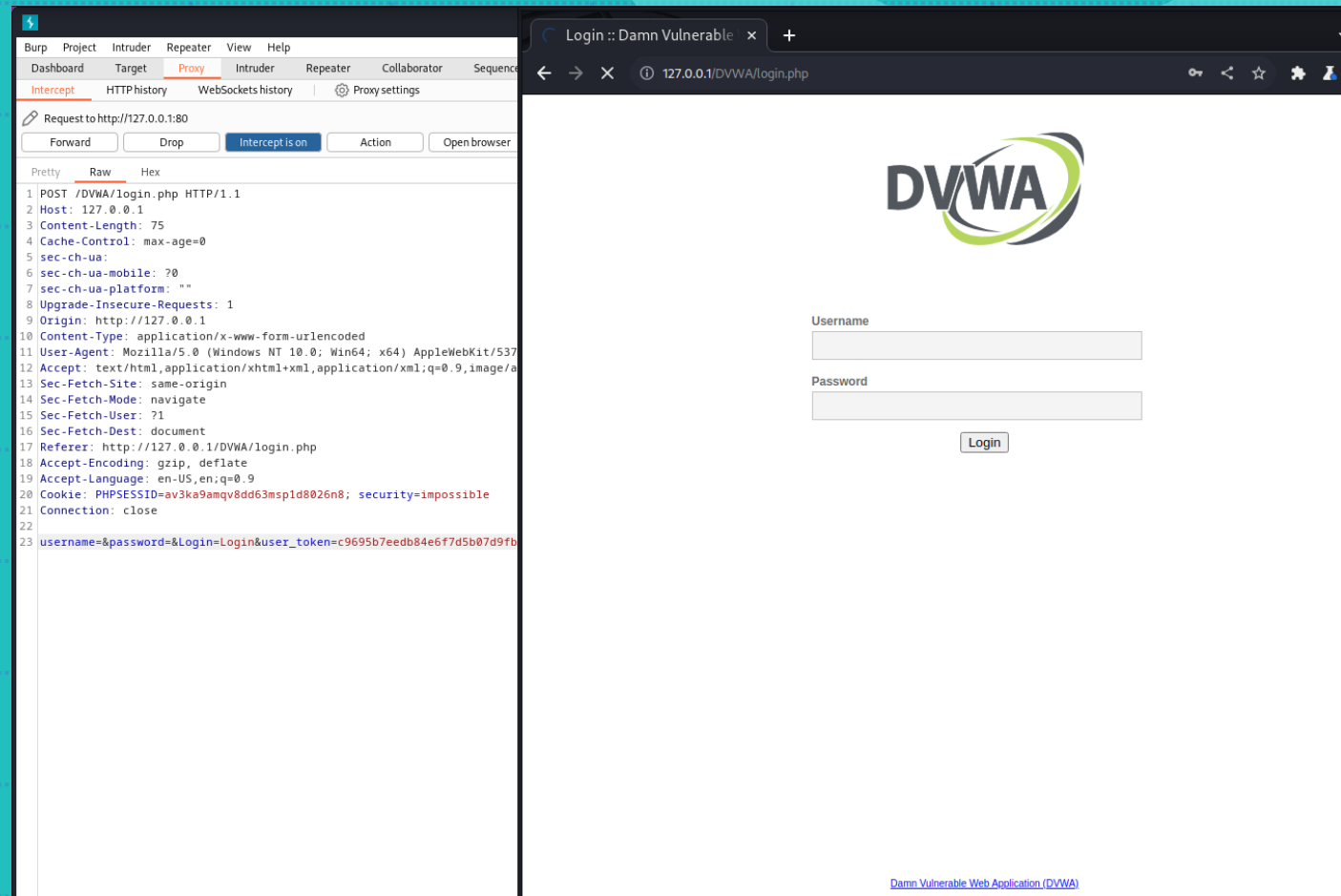
The screenshot shows a web browser window on the left and an HTTP response viewer on the right. The browser's address bar shows a URL ending in `/1.1`. The page content includes a login form with a password field and a submit button labeled "Login". Below the form, a message box displays "Login failed". The browser's user agent string is visible: `(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171`. The response viewer on the right shows the raw HTML of the page, with the "Login failed" message highlighted by a red underline. The response is a 200 OK status.

```
200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 1024
Server: Apache/2.4.18 (Ubuntu)
Date: Mon, 10 Jun 2024 10:10:10 GMT
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Set-Cookie: PHPSESSID=amqv8dd63msp1d8026n8; security=impossible

<?php
// ...
</label>
<input type="password" class="loginInput" AUTOCOMPLE
<br />
<br />
<p class="submit">
  <input type="submit" value="Login" name="Login">
</p>
</fieldset>
<input type='hidden' name='user_token' value='3c68a1bb1
</form>
<br />
<div class="message">
  Login failed
</div>
<br />
<br />
<br />
<br />
<br />
<br />
<br />
</div >
<!--<div id="content">-->
<div id="footer">
```

Altra opzione

Al contrario si può anche accedere al web andando ad inserire nell'ultima riga del codice su Burp, le credenziali username e password corrette. Procedendo ci permetterà di effettuare l'accesso al sito senza farlo direttamente con il motore di ricerca.





Fine del progetto

Amedeo Natalizi