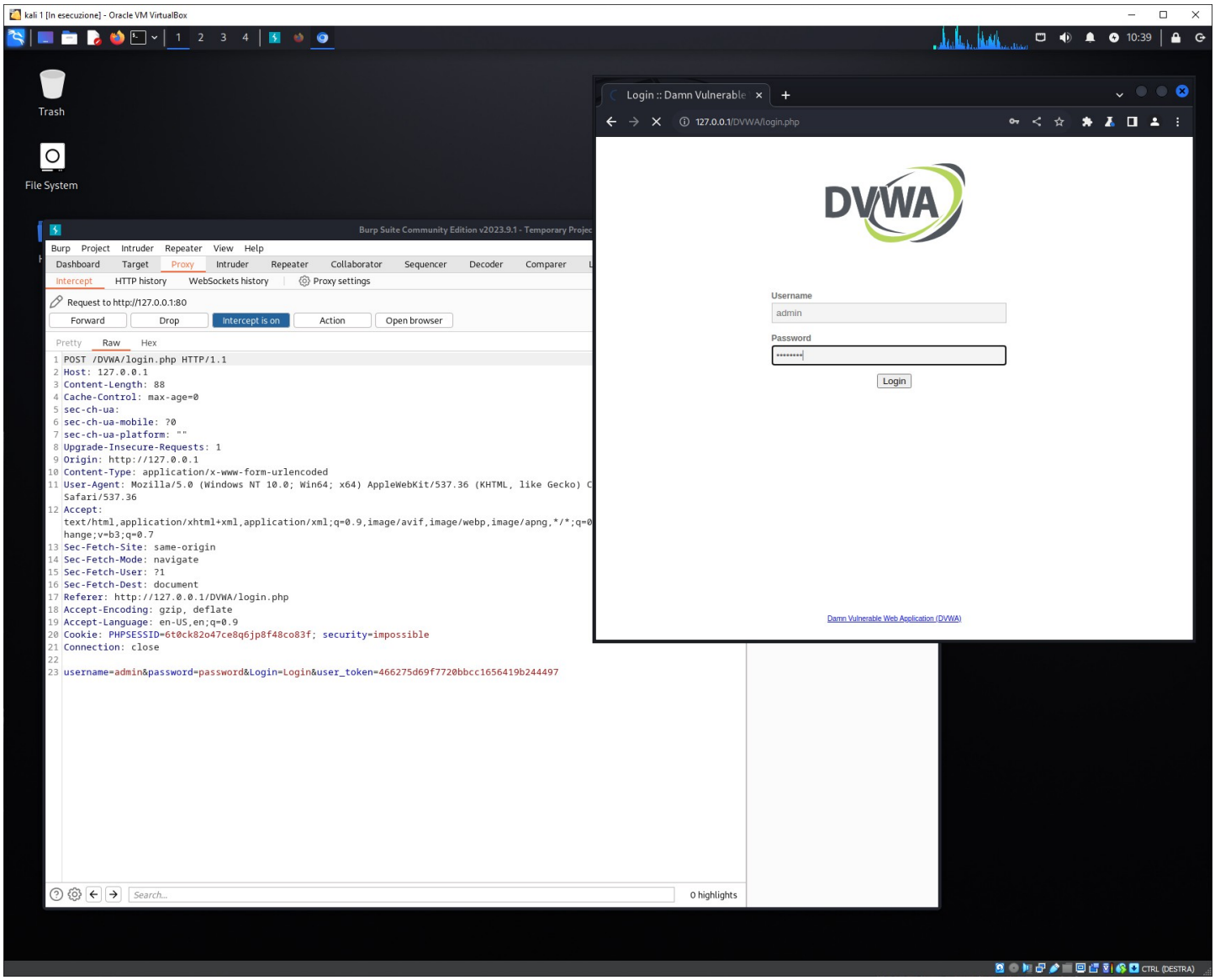
Esercizio Web Application – preparazione ambiente

Burpsuite è uno degli strumenti più utilizzati in ambito web app.
Burpsuite è un intercepting proxy, uno strumento che permette di analizzare e modificare le richieste e le risposte scambiate in un modello client-server

Operazioni che può fare:

- Intercettare le richieste e le risposte tra il browser e il server web.
- Costruire e modificare richieste ad hoc manualmente per testare le risposte di un applicativo.
- Inviare richieste malformate ad un server per studiare la risposta.
- Indicizzare tutti i percorsi di un sito visitando automaticamente la pagine, e inviando risposta positiva per le sole pagine esistenti.

Lanciamo Burpsuite, scegliamo un progetto temporaneo ed apriamo un browser, inserendo l'indirizzo della nostra DVWA: 1270.0.1/DVWA e inseriamo nei campi login e password i valori «admin» e «password» rispettivamente.



Proviamo a modificare i campi, ed inviare la richiesta inserendo delle credenziali sicuramente errate.

```
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=ri3flanbej4outqgcikk4kp0h7; security=impossible
21 Connection: close
22
23 username=oma&password=omar&Login=Login&user_token=ce0de8c8e0eba69921a0780f1ff74090
```

Come ci aspettavamo con le credenziali errate non riusciamo ad entrare. Ne abbiamo evidenza nel body della http response dove leggiamo «Login failed». Riga 63.

Qui sotto la response al completo:

Pretty Raw Hex \n

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
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/119.0.6045.159 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, br
17 Accept-Language: en-US,en;q=0.9
18 Cookie: PHPSESSID=ri3flanbej4outqgcikk4kp0h7; security=impossible
19 Connection: close
20
21
```

```
      <!--<div id="header">-->

    <div id="content">

      <form action="login.php" method="post">

        <fieldset>

          <label for="user">
            Username
          </label>
           <input type="text" class="loginInput" size="20" name="username">
          <br />


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

          <br />

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

        </fieldset>

        <input type='hidden' name='user_token' value='ed0dc6505c24611e6ad38022082e27e3' />

      </form>

      <br />

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

      <br />
      <br />
      <br />
      <br />
      <br />
      <br />
      <br />
      <br />
```