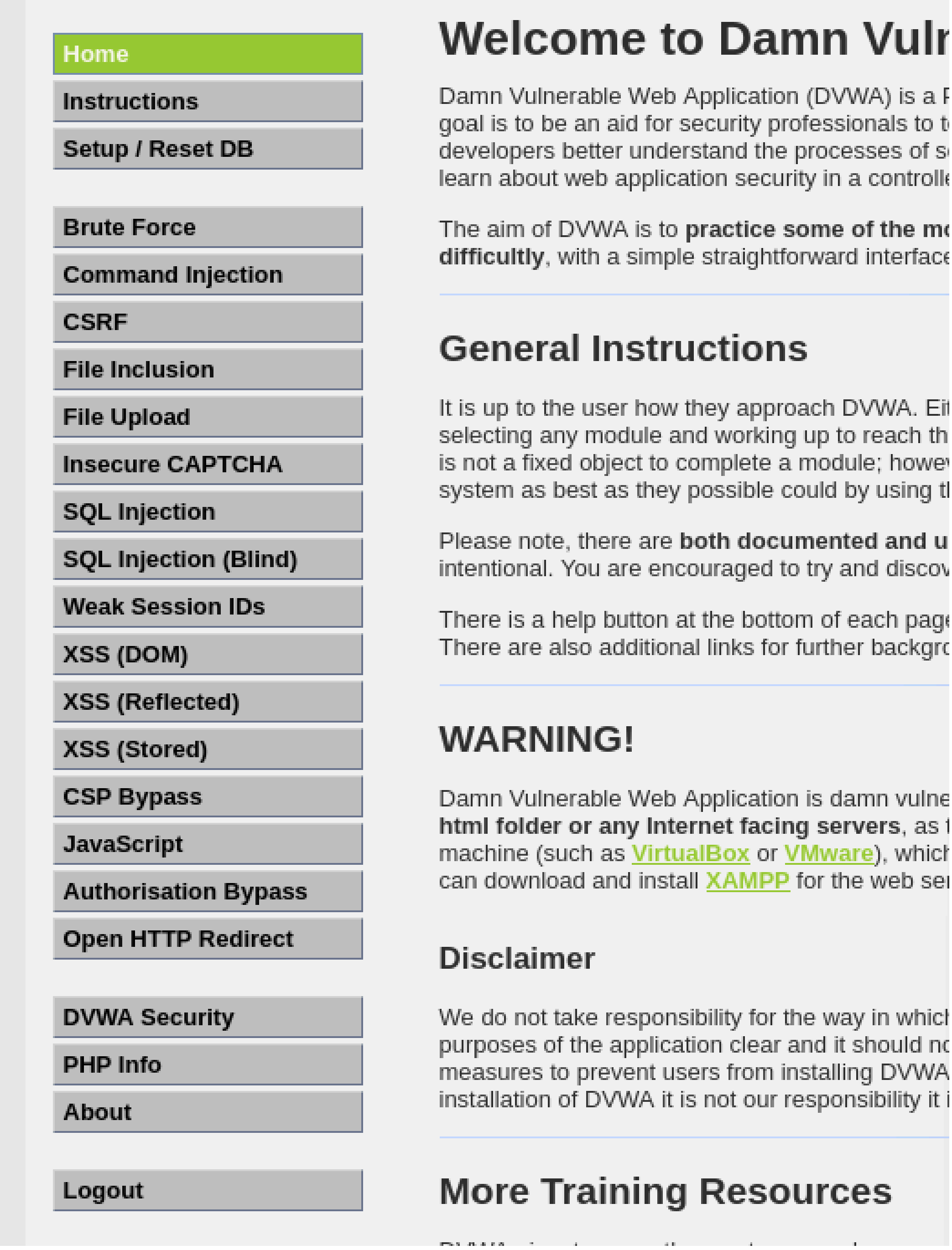


Welcome to Damn Vulr

Damn Vulnerable Web Application (DVWA) is a F
goal is to be an aid for security professionals to t
developers better understand the processes of s
learn about web application security in a controlle

The aim of DVWA is to **practice some of the mo
difficultly**, with a simple straightforward interface

General Instructions

It is up to the user how they approach DVWA. Eit
selecting any module and working up to reach th
is not a fixed object to complete a module; howev
system as best as they possible could by using t

Please note, there are **both documented and u**
intentional. You are encouraged to try and discov

There is a help button at the bottom of each page
There are also additional links for further backgro

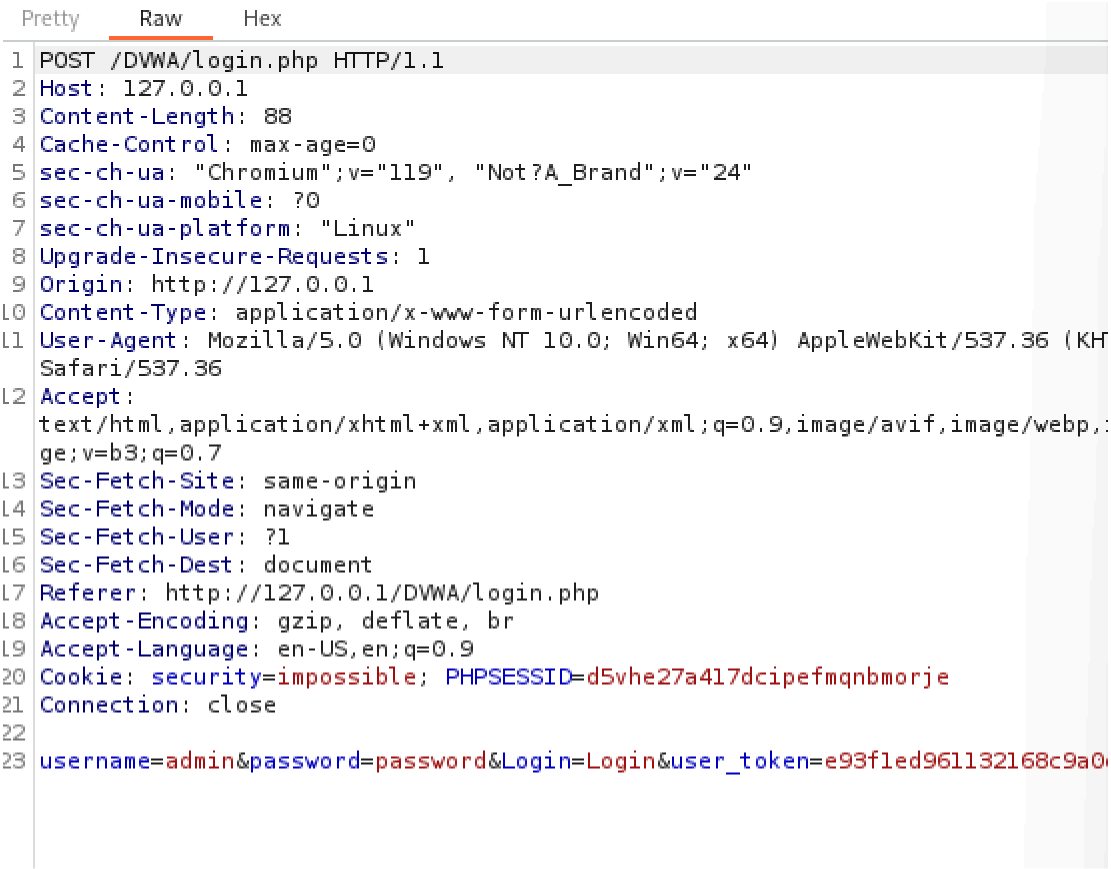
WARNING!

Damn Vulnerable Web Application is damn vulne
html folder or any Internet facing servers, as t
machine (such as VirtualBox or VMware), which
can download and install XAMPP for the web ser

Disclaimer

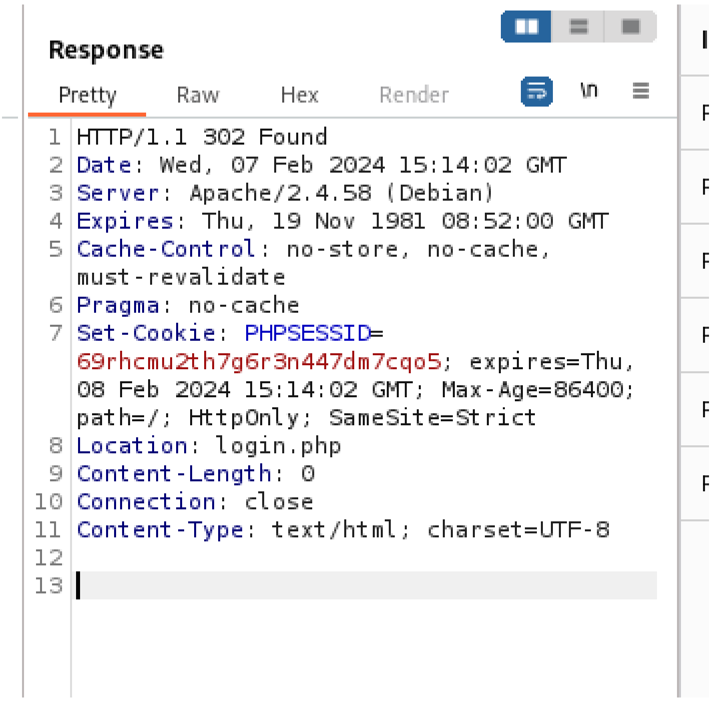
We do not take responsibility for the way in which
purposes of the application clear and it should no
measures to prevent users from installing DVWA
installation of DVWA it is not our responsibility it i

More Training Resources



```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
ge;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=impossible; PHPSESSID=d5vhe27a417dcipefmqnbmorje
Connection: close

username=admin&password=password&Login=Login&user_token=e93f1ed961132168c9a0
```



```
HTTP/1.1 302 Found
Date: Wed, 07 Feb 2024 15:14:02 GMT
Server: Apache/2.4.58 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=
69rhcmu2th7g6r3n447dm7cqo5; expires=Thu,
08 Feb 2024 15:14:02 GMT; Max-Age=86400;
path=/; HttpOnly; SameSite=Strict
Location: login.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

```