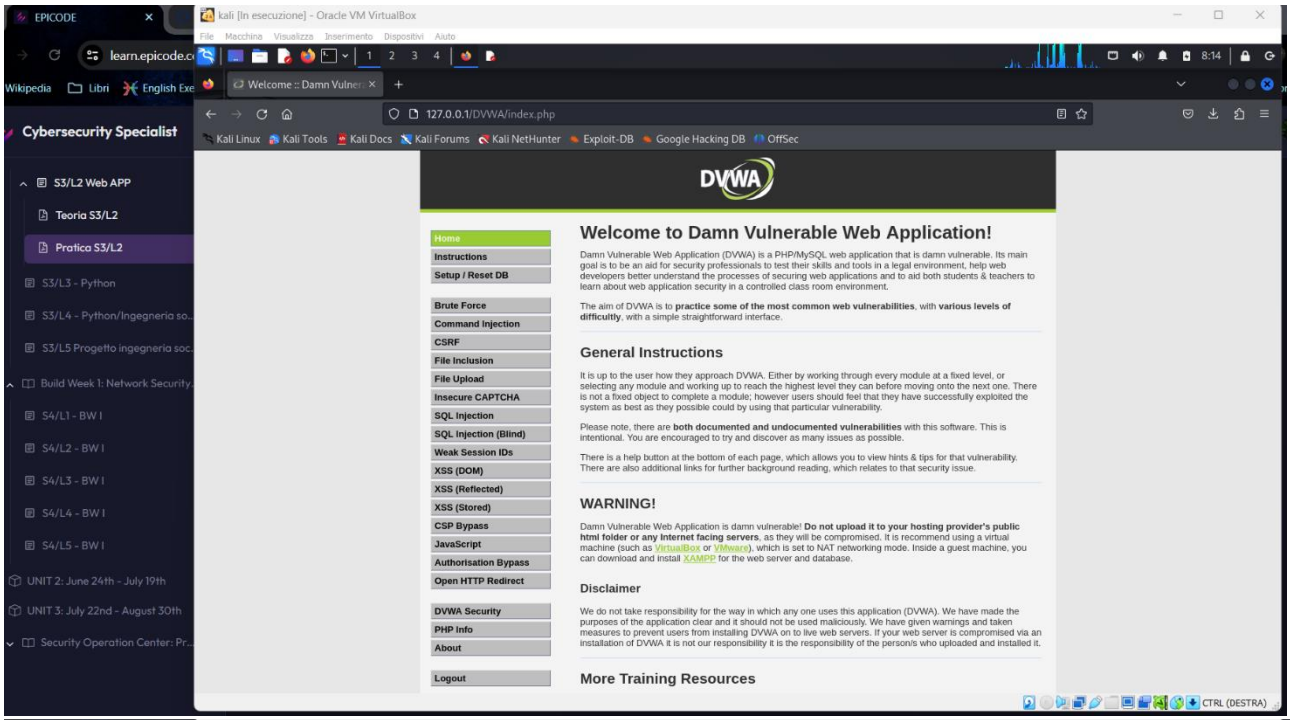
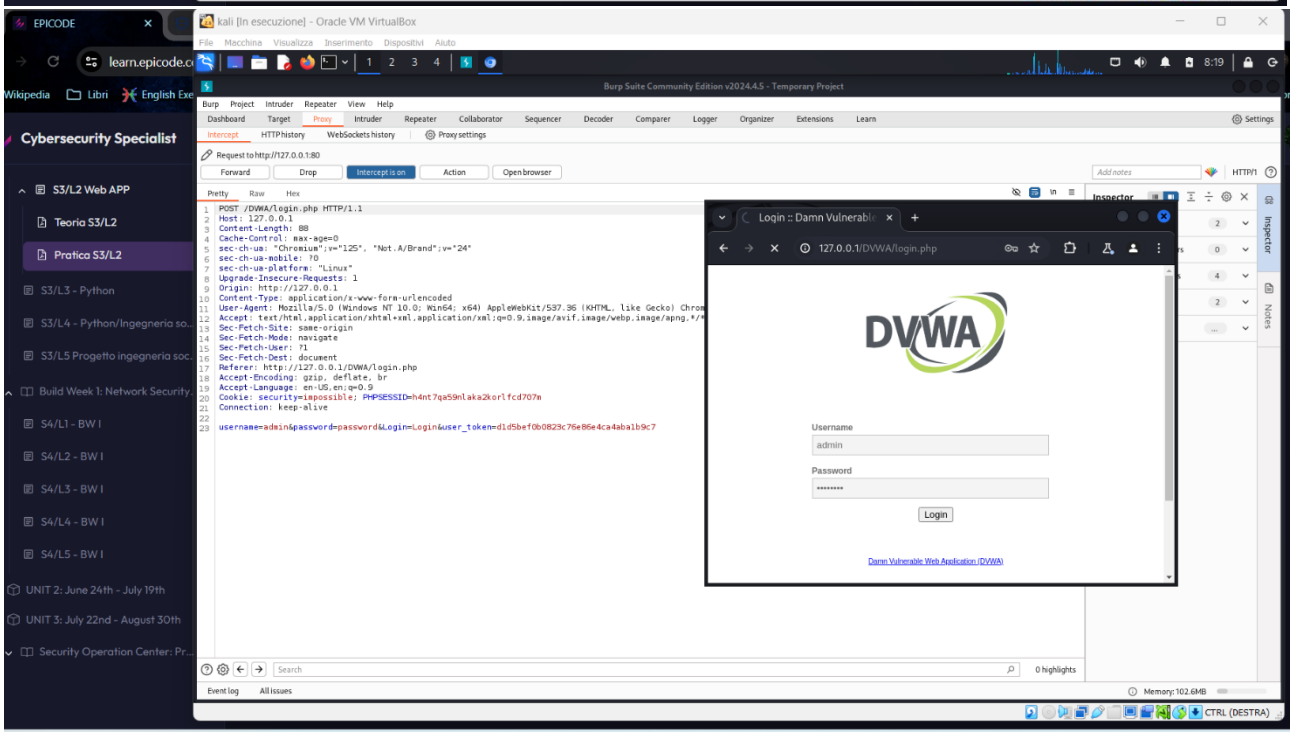
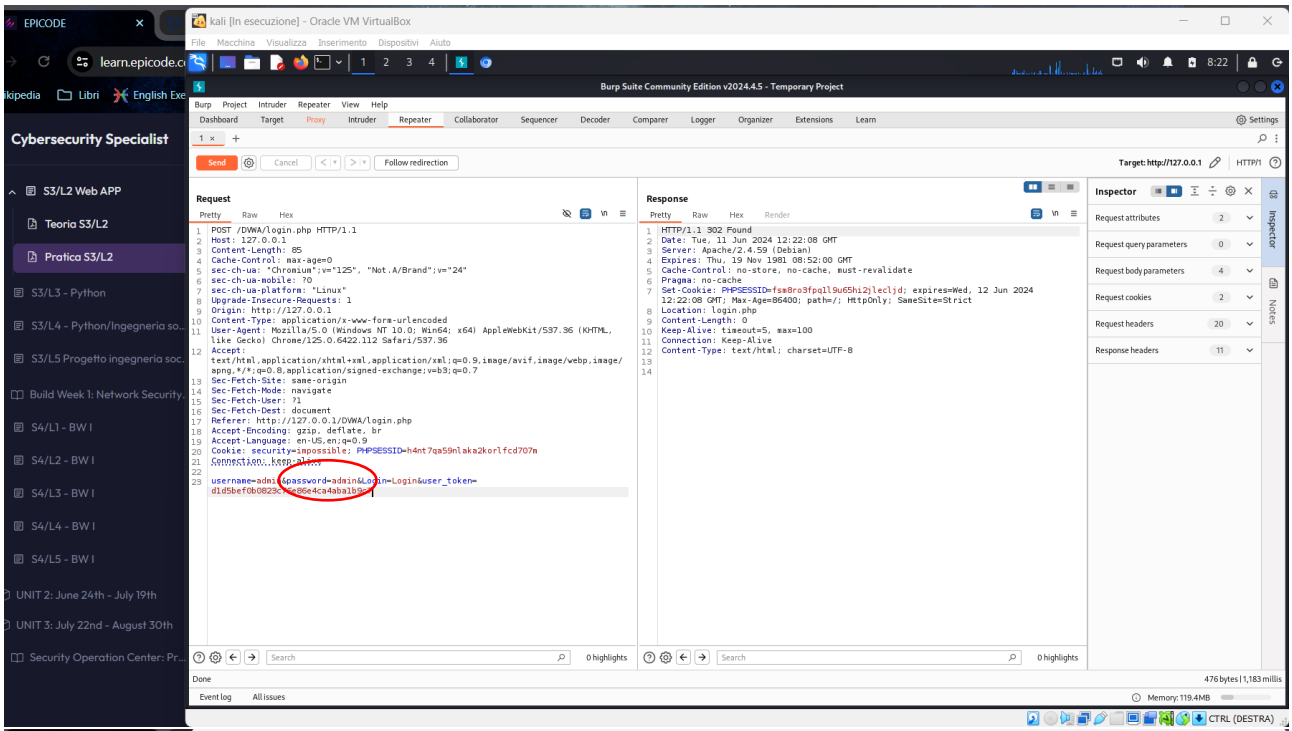
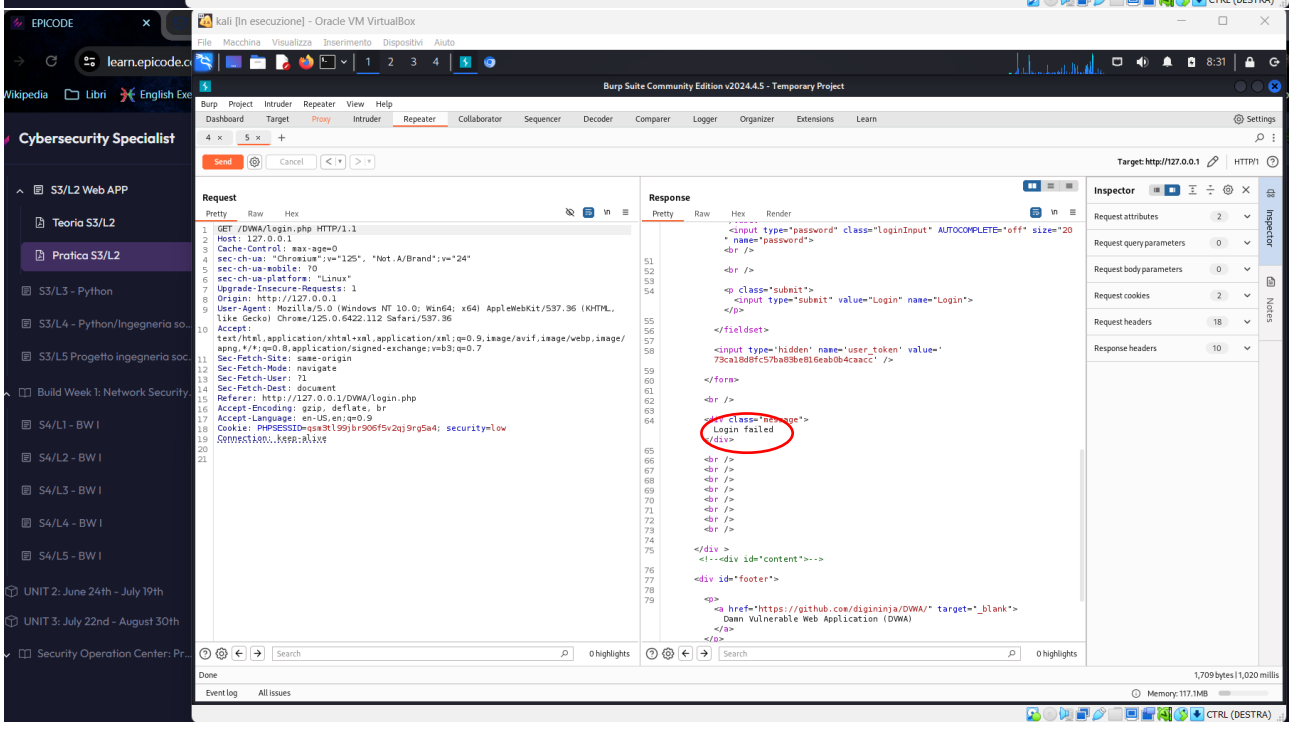

EPICODE
learn.epicode.c
Wikipedia
Libri
English Exe
Cybersecurity Specialist
S3/L2 Web APP
Teoria S3/L2
Pratica S3/L2
S3/L3 - Python
S3/L4 - Python/Ingegneria so...
S3/L5 Progetto ingegneria soc...
Build Week 1: Network Security...
S4/L1 - BW I
S4/L2 - BW I
S4/L3 - BW I
S4/L4 - BW I
S4/L5 - BW I
UNIT 2: June 24th - July 19th
UNIT 3: July 22nd - August 30th
Security Operation Center: Pr...
kali [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Welcome :: Damn Vulner...
127.0.0.1/DVWA/index.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Welcome to Damn Vulnerable Web Application!
Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.
The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficultly, with a simple straightforward interface.
General Instructions
It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.
Please note, there are both documented and undocumented vulnerabilities with this software. This is intentional. You are encouraged to try and discover as many issues as possible.
There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.
WARNING!
Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.
Disclaimer
We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
More Training Resources
CTRL (DESTRA)


EPICODE
learn.epicode.c
Wikipedia
Libri
English Exe
Cybersecurity Specialist
S3/L2 Web APP
Teoria S3/L2
Pratica S3/L2
S3/L3 - Python
S3/L4 - Python/Ingegneria so...
S3/L5 Progetto ingegneria soc...
Build Week 1: Network Security...
S4/L1 - BW I
S4/L2 - BW I
S4/L3 - BW I
S4/L4 - BW I
S4/L5 - BW I
UNIT 2: June 24th - July 19th
UNIT 3: July 22nd - August 30th
Security Operation Center: Pr...
kali [In esecuzione] - Oracle VM VirtualBox
Burp Suite Community Edition v2024.4.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://127.0.0.1:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
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="125", "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 (KHTML, like Gecko) Chrom
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
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=h4nt7qa59nlaka2korlfcd707m
Connection: keep-alive
username=admin&password=password&Login=Login&user_token=d1d5bef0b0823c76e86e4ca4ba1b9c7
Login :: Damn Vulnerable
127.0.0.1/DVWA/login.php
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA)
Inspector
Notes
Search
0 highlights
Event log All issues
Memory: 102.6MB
CTRL (DESTRA)


kali [In esecuzione] - Oracle VM VirtualBox
Burp Suite Community Edition v2024.4.5 - Temporary Project
Request
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 85
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="125", "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 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36
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
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=h4nt7qa59nlaka2korlfcd707m
Connection: keep-alive
username=admin&password=admin&Login=Login&user_token=
d1d5bef0b0823c7ea86e4ca4aba1b9c7
Response
HTTP/1.1 302 Found
Date: Tue, 11 Jun 2024 12:22:08 GMT
Server: Apache/2.4.59 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=fsm8ro3fpqll9u65hi2jlecljd; expires=Wed, 12 Jun 2024 12:22:08 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
Location: login.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers
Cybersecurity Specialist
S3/L2 Web APP
Teoria S3/L2
Pratica S3/L2
S3/L3 - Python
S3/L4 - Python/Ingegneria so...
S3/L5 Progetto ingegneria soc...
Build Week 1: Network Security...
S4/L1 - BW I
S4/L2 - BW I
S4/L3 - BW I
S4/L4 - BW I
S4/L5 - BW I
UNIT 2: June 24th - July 19th
UNIT 3: July 22nd - August 30th
Security Operation Center: Pr...


kali [In esecuzione] - Oracle VM VirtualBox
Burp Suite Community Edition v2024.4.5 - Temporary Project
Request
GET /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="125", "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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36
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
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: PHPSESSID=qsm3tl99jbr9O6f5v2qj9rg5a4; security=low
Connection: keep-alive
Response
<input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="password">

<input type="submit" value="Login" name="Login">

</fieldset>
<input type='hidden' name='user_token' value='73ca18d8fc57ba83be816eab0b4caacc' />
</form>

Login failed

<!--<div id="content">-->

Damn Vulnerable Web Application (DVWA)

Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers
Cybersecurity Specialist
S3/L2 Web APP
Teoria S3/L2
Pratica S3/L2
S3/L3 - Python
S3/L4 - Python/Ingegneria so...
S3/L5 Progetto ingegneria soc...
Build Week 1: Network Security...
S4/L1 - BW I
S4/L2 - BW I
S4/L3 - BW I
S4/L4 - BW I
S4/L5 - BW I
UNIT 2: June 24th - July 19th
UNIT 3: July 22nd - August 30th
Security Operation Center: Pr...