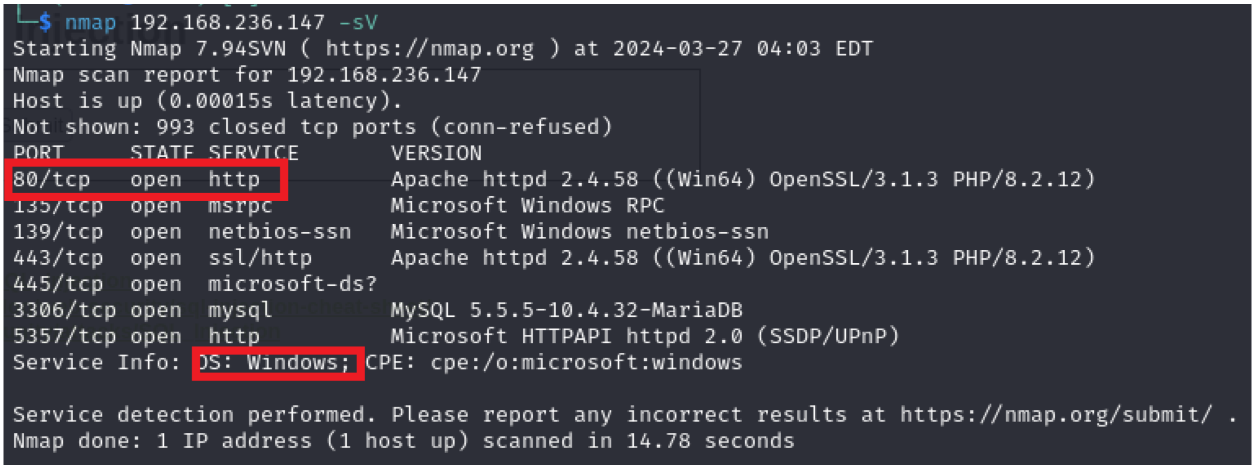
認證失效

資訊收集



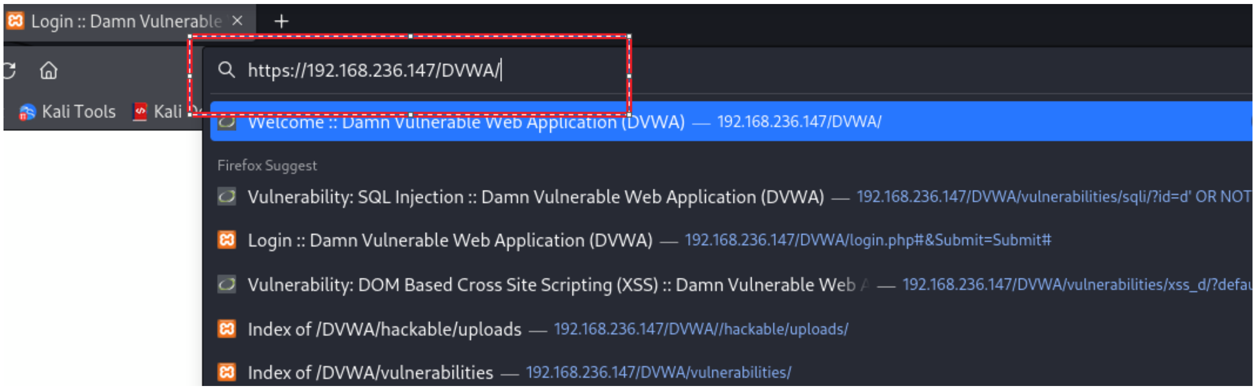
```
└─$ nmap 192.168.236.147 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 04:03 EDT
Nmap scan report for 192.168.236.147
Host is up (0.00015s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http      Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MySQL 5.5.5-10.4.32-MariaDB
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.78 seconds
```

發現80 端口開啟 系統為Windows

偵查

在URL輸入https://192.168.236.147/DVWA/



https://192.168.236.147/DVWA/

Welcome :: Damn Vulnerable Web Application (DVWA) — 192.168.236.147/DVWA/

Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) — 192.168.236.147/DVWA/vulnerabilities/sqli/?id=d' OR NOT

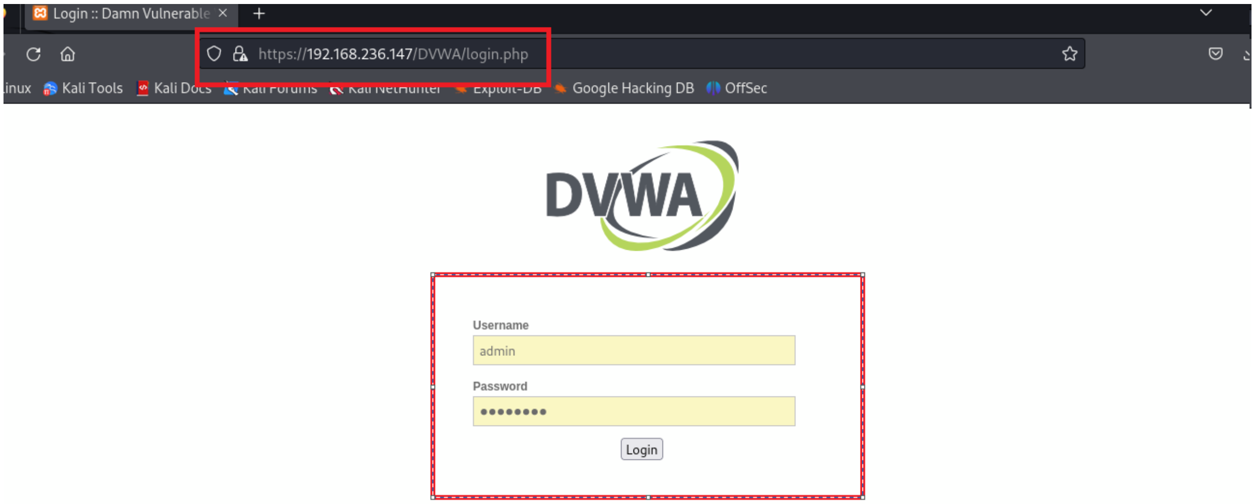
Login :: Damn Vulnerable Web Application (DVWA) — 192.168.236.147/DVWA/login.php#&Submit=Submit#

Vulnerability: DOM Based Cross Site Scripting (XSS) :: Damn Vulnerable Web — 192.168.236.147/DVWA/vulnerabilities/xss_d/?defau

Index of /DVWA/hackable/uploads — 192.168.236.147/DVWA//hackable/uploads/

Index of /DVWA/vulnerabilities — 192.168.236.147/DVWA/vulnerabilities/

發現被導向https://192.168.236.147/DVWA/login.php



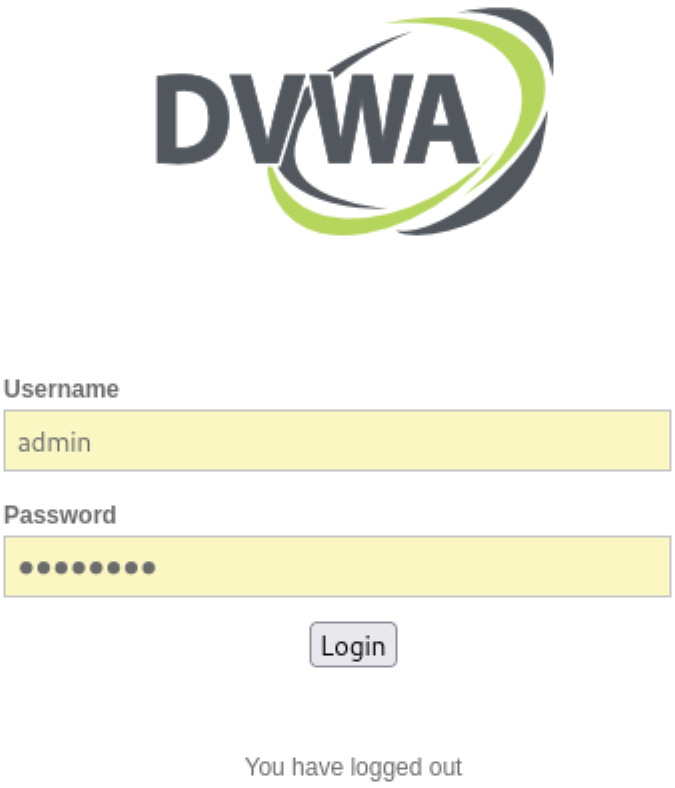
https://192.168.236.147/DVWA/login.php

Username: admin

Password: ••••••••

漏洞利用

嘗試使用admin/password 若密碼登入



Username

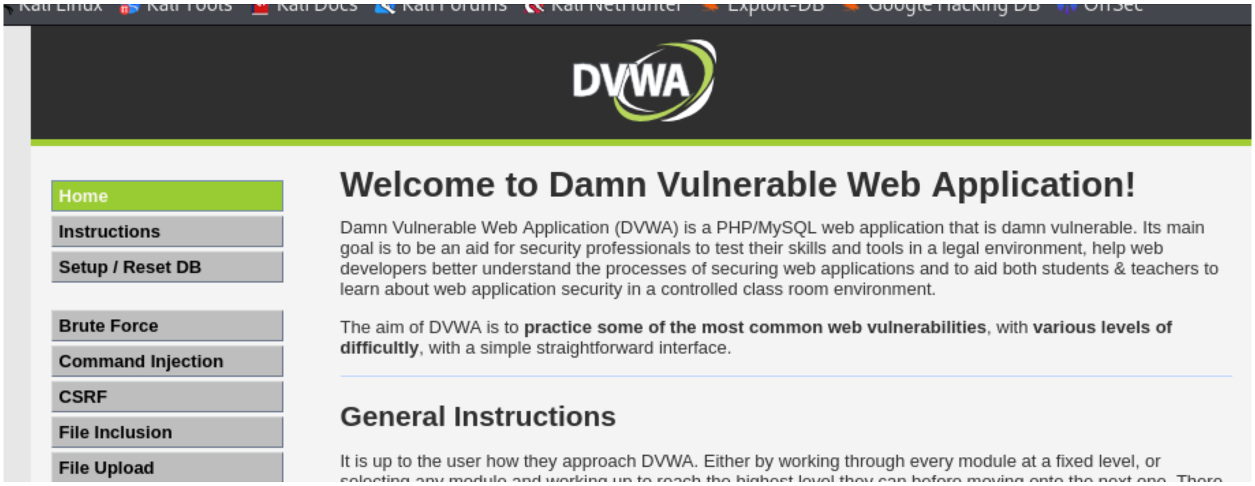
admin

Password

●●●●●●●●

You have logged out

成功



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