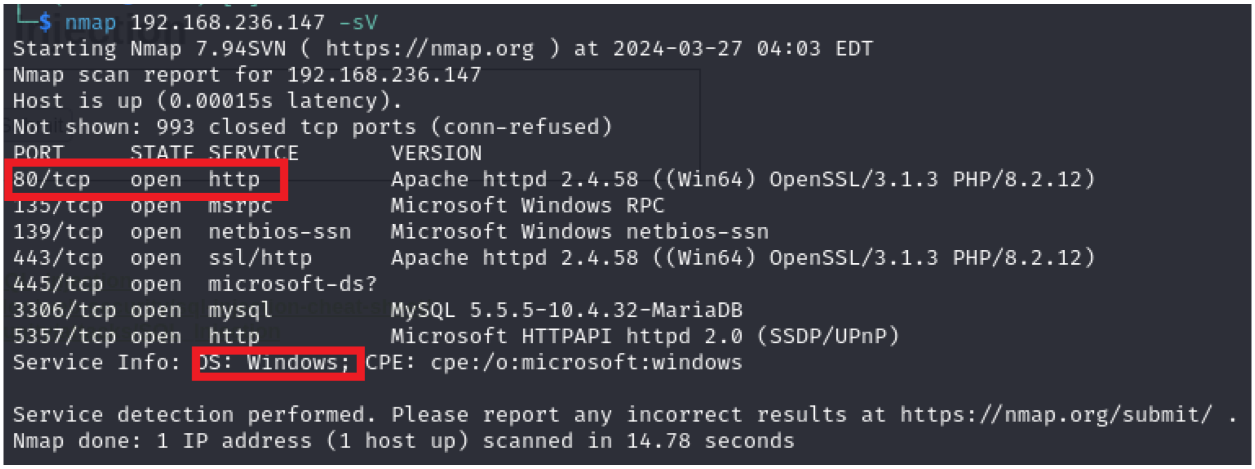
XSS

資訊收集



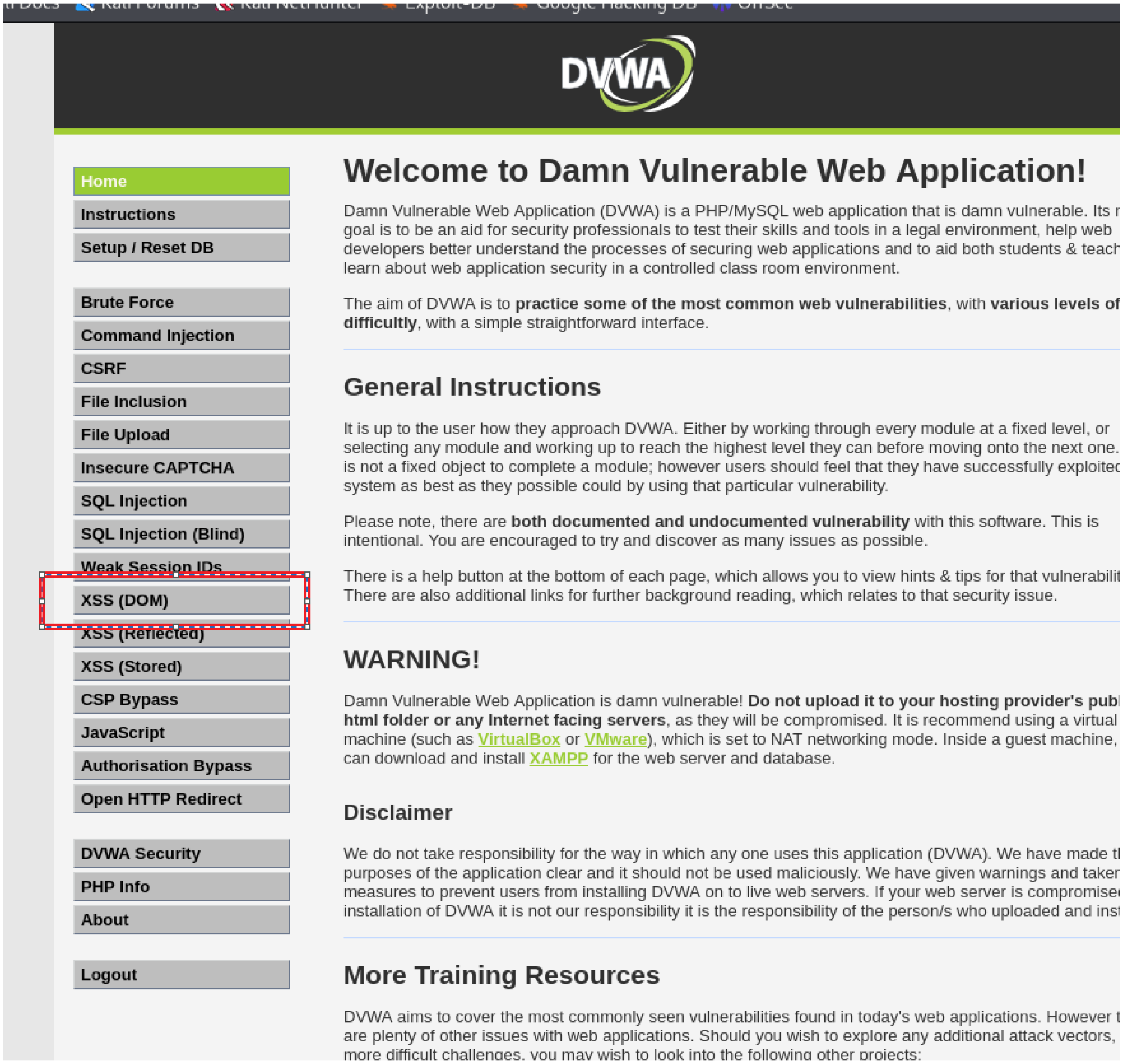
```
└─$ nmap 192.168.236.147 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 04:03 EDT
Nmap scan report for 192.168.236.147
Host is up (0.00015s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.58 ((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

點擊XSS(DOM)



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its r 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 & teach 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. is not a fixed object to complete a module; however users should feel that they have successfully exploited system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** 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 vulnerabilit 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 publ 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, can download and install XAMPP for the web server and database.

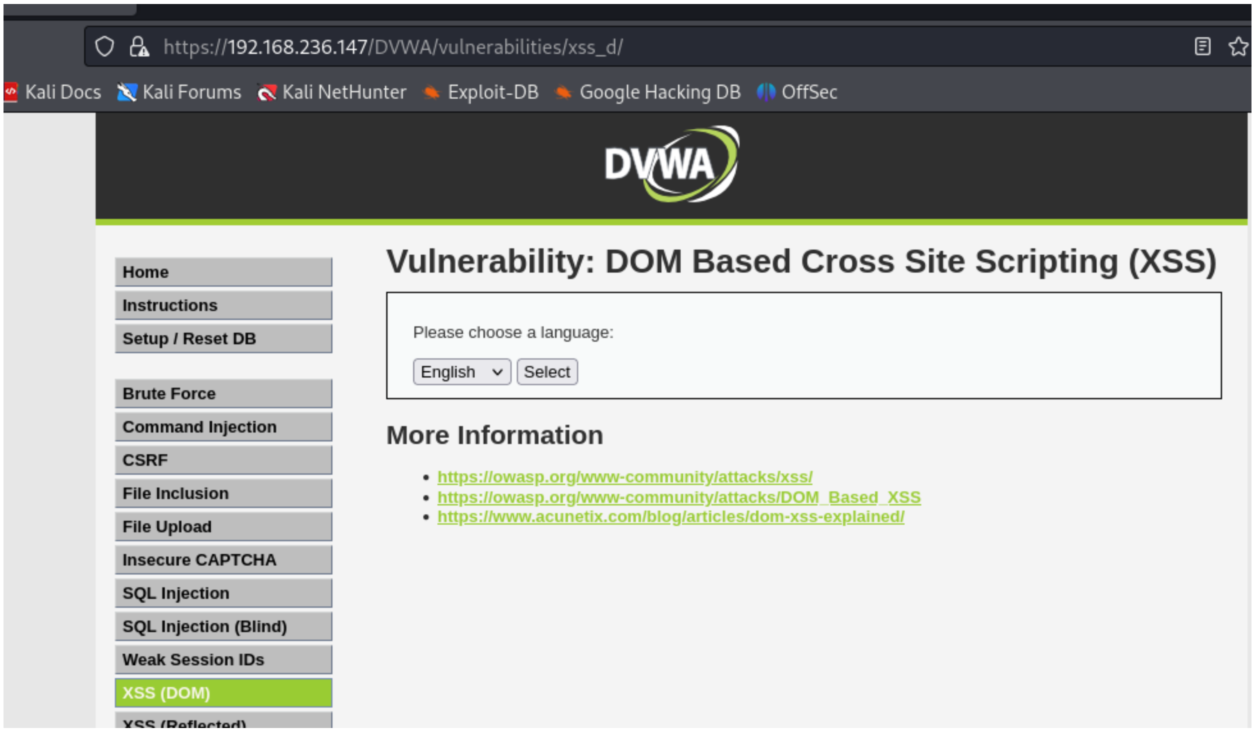
Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made tl 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 installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and inst

More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However t are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, more difficult challenges, you may wish to look into the following other projects:

被導向https://192.168.236.147/DVWA/vulnerabilities/xss_d/



https://192.168.236.147/DVWA/vulnerabilities/xss_d/

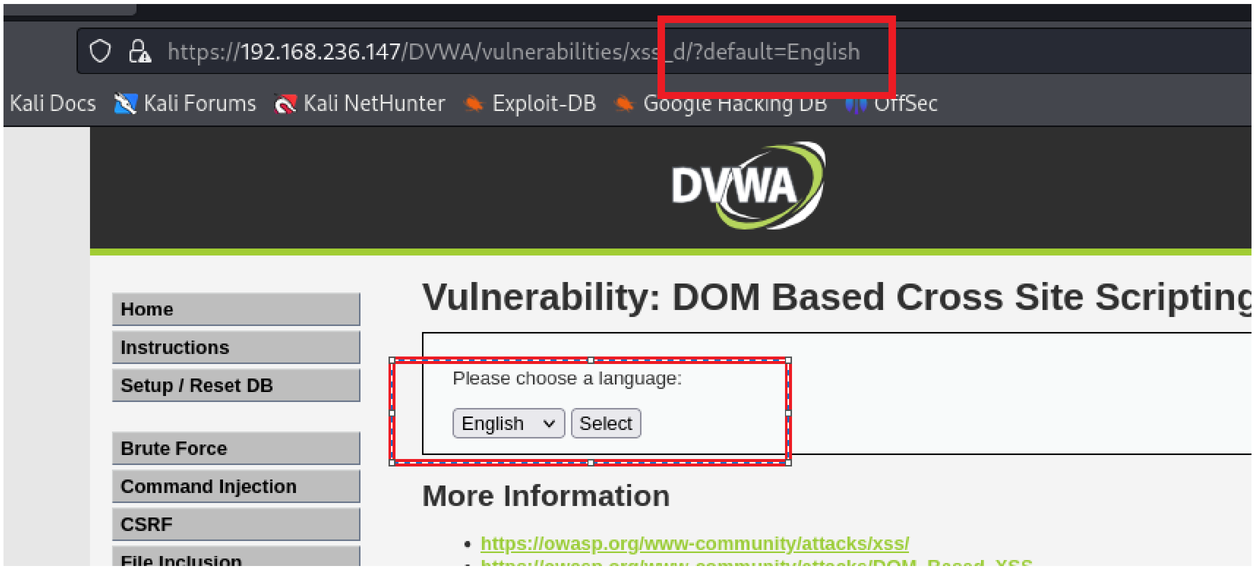
Vulnerability: DOM Based Cross Site Scripting (XSS)

Please choose a language:

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/attacks/DOM_Based_XSS
- https://www.acunetix.com/blog/articles/dom-xss-explained/

嘗試輸入English並送出



https://192.168.236.147/DVWA/vulnerabilities/xss_d/?default=English

Vulnerability: DOM Based Cross Site Scripting

Please choose a language:

More Information

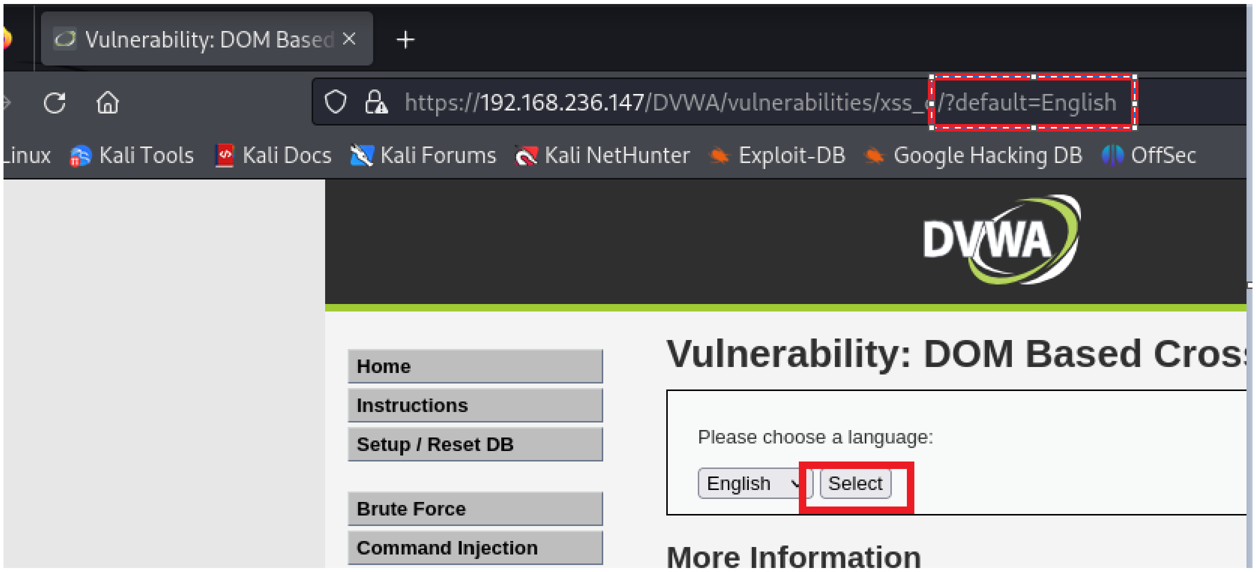
- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/attacks/DOM_Based_XSS

發先URL顯示default=English

漏洞利用

嘗試輸入English並送出

發現default=English



https://192.168.236.147/DVWA/vulnerabilities/xss_d/?default=English

Vulnerability: DOM Based Cros

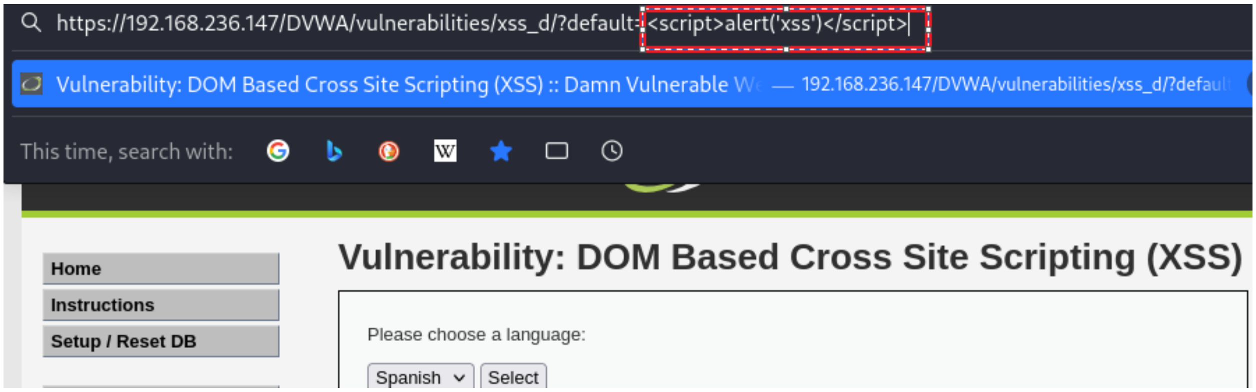
Please choose a language:

English Select

More Information

嘗試在URL 輸入XSS指令:

<script>alert('xss')</script>



https://192.168.236.147/DVWA/vulnerabilities/xss_d/?default=<script>alert('xss')</script>

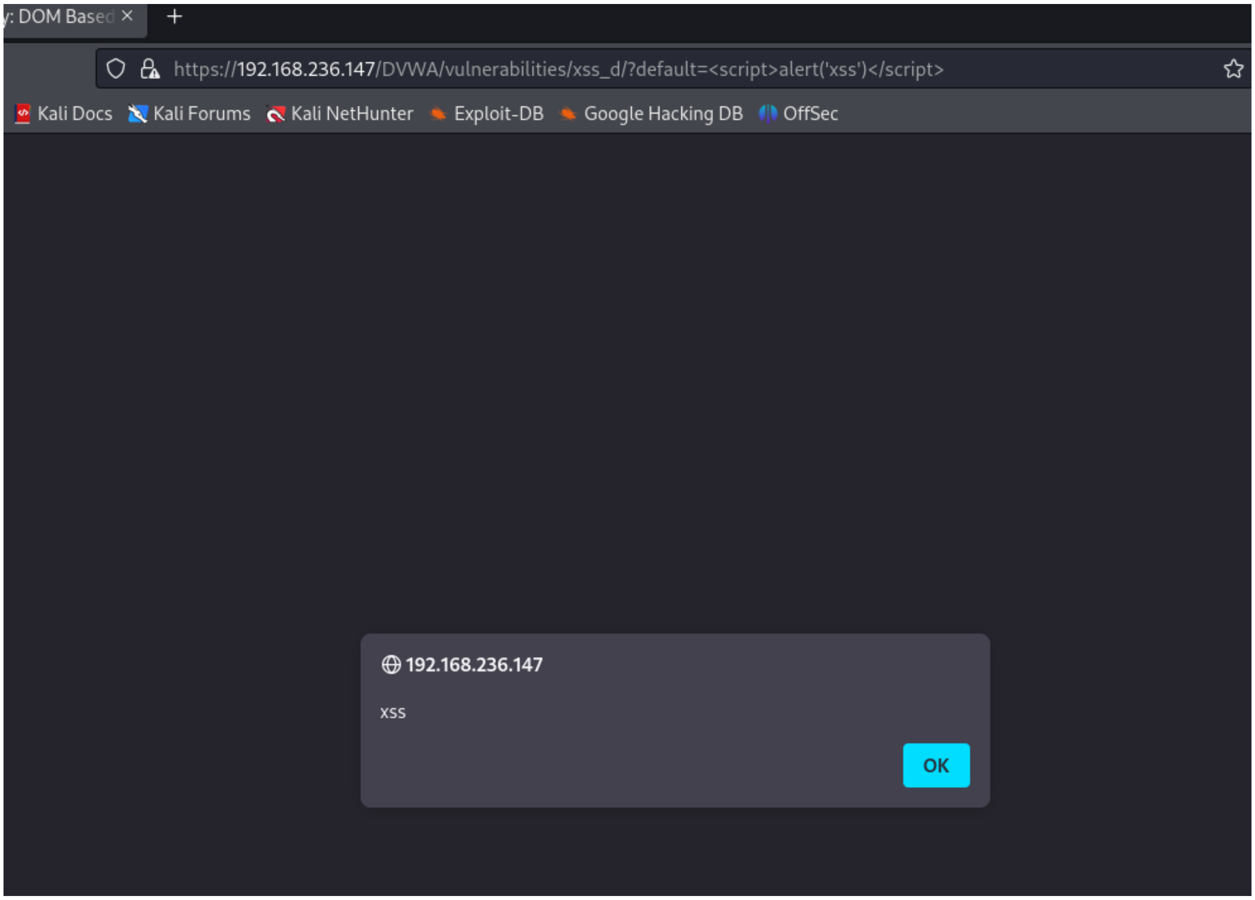
Vulnerability: DOM Based Cross Site Scripting (XSS) :: Damn Vulnerable W — 192.168.236.147/DVWA/vulnerabilities/xss_d/?defaul

Vulnerability: DOM Based Cross Site Scripting (XSS)

Please choose a language:

Spanish Select

XSS 成功



y: DOM Based
https://192.168.236.147/DVWA/vulnerabilities/xss_d/?default=<script>alert('xss')</script>
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
192.168.236.147
xss
OK