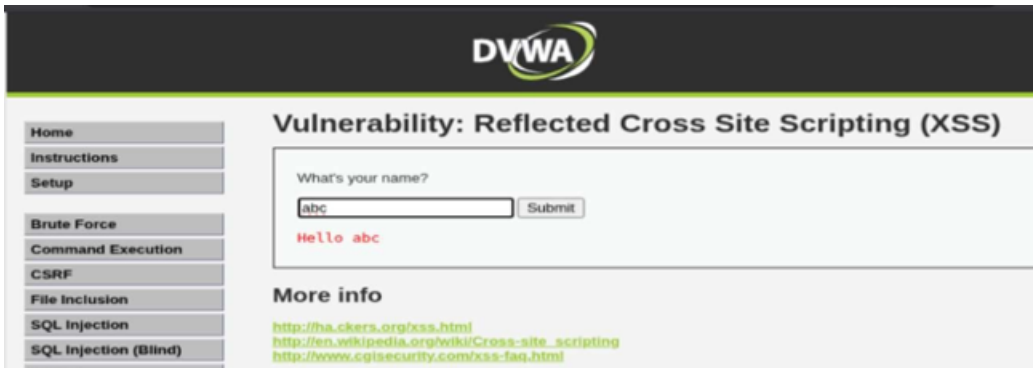
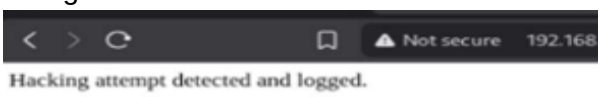
VAPT 3rd Report

1 – Advanced Exploitation and Web Application Testing Lab

Target: http://192.168.0.125/dvwa
Tools: Nmap, Owasp ZAP, Nikto



XSS – generating remote alert



XSS - inserting script to retrieve cookies

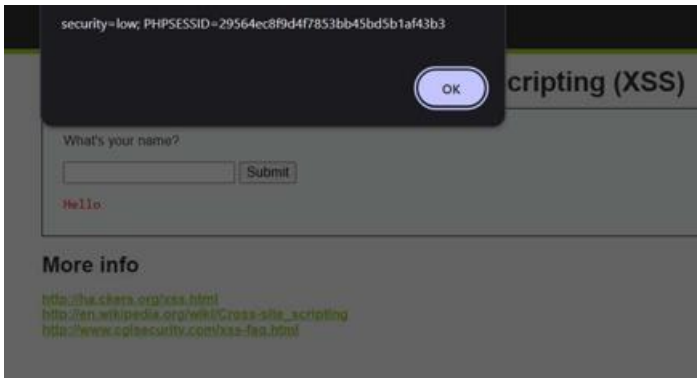
Vulnerability	Severity	URL
Remote Code Execution - CVE2012-1823	High	http://192.168.0.125/dvwa/?d+allow_url_include%3d1+d+auto_prepend_file%3dphp://input

		http://192.168.0.125/dvwa/login.php?d+allow_url_include%3d1+d+auto_prepend_file%3dphp://input
Source Code Disclosure - CVE2012-1823	High	http://192.168.0.125/dvwa/?-s
		http://192.168.0.125/dvwa/login.php?-s
Content Security Policy (CSP) Header Not Set	Medium	http://192.168.0.125/dvwa
		http://192.168.0.125/dvwa/login.php
		http://192.168.0.125/robots.txt
		http://192.168.0.125/sitemap.xml
Directory Browsing	Medium	http://192.168.0.125/dvwa/dvwa/
		http://192.168.0.125/dvwa/dvwa/css/
		http://192.168.0.125/dvwa/dvwa/images/
Hidden File Access	Medium	http://192.168.0.125/phpinfo.php
Missing Anti-clickjacking Header	Medium	http://192.168.0.125/dvwa
		http://192.168.0.125/dvwa/login.php
Cookie No HttpOnly Flag	Low	http://192.168.0.125/dvwa/
Cookie without SameSite Attribute	Low	http://192.168.0.125/dvwa/
Server Leaks via "X-PoweredBy" HTTP Response Header Field(s)	Low	http://192.168.0.125/dvwa
		http://192.168.0.125/dvwa/login.php
Server Leaks via "Server" HTTP Response Header Field	Low	http://192.168.0.125/dvwa
		http://192.168.0.125/dvwa/
		http://192.168.0.125/dvwa/dvwa/css/login. css

		http://192.168.0.125/dvwa/dvwa/images/l ogin_logo.png
		http://192.168.0.125/dvwa/dvwa/images/R andomStorm.png
		http://192.168.0.125/dvwa/login.php
		http://192.168.0.125/robots.txt
		http://192.168.0.125/sitemap.xml
		http://192.168.0.125/dvwa/login.php

2 – Post-Exploitation Evidence collection

Alert generated on the web



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.