## Lab 12: Web Application Vulnerability Scanning with Nikto

**Scenario**

CyberSecure Labs, a leading cybersecurity services provider, has been commissioned by InfoTech Retail, an e-commerce company specializing in online sales, to evaluate the security of its customer-facing web applications. Since the platform processes sensitive customer information such as payment details, account credentials, and personal data, ensuring the confidentiality, integrity, and availability of its web infrastructure is a top priority. During the initial security audit, the client expresses concern about potential risks stemming from outdated software components, misconfigured servers, and common web vulnerabilities that attackers could exploit to compromise the application. To address these concerns, the security team decides to use Nikto, an open-source web server scanner, to perform an in-depth vulnerability assessment of the target web application under controlled conditions.

**Solution**

As a certified cybersecurity practitioner, your task is to conduct a vulnerability scan against the target web server using Nikto. Begin by launching Nikto from the terminal and specifying the target URL of the web application. Nikto will automatically test for thousands of known issues, including outdated server versions, default files, insecure configurations, and potential injection points. Carefully review the scan results to identify critical findings such as the presence of outdated Apache modules, directory listing exposures, or vulnerabilities to Cross-Site Scripting (XSS) and SQL injection attacks.

Nikto is an open source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and versions specific problems on over 270 servers. It also checks for server configuration items such as multiple index files and HTTP server options. It will attempt to identify installed web servers and software.

|  |
| --- |
| 1. On the **ParrotOS** machine, click the **Applications** menu in the top-left corner of the **Desktop** and navigate to **Pentesting > Web Application Analysis > Web Vulnerability Scanners > nikto** to open Nikto in the **Terminal** window.    2. A Parrot Terminal window appears. Type your **password** in the **[sudo] password for attacker** field and press **Enter**. Nikto initializes.    3. Nikto scanning options will be displayed to scan the target website.    4. You can further type **nikto -H** and press **Enter** to view various available commands with full help text.    5. The result appears, displaying various available options in Nikto. We will use the **Tuning** option to do a more comprehensive scan of the target web server.    6. Execute the command **nikto -h www.certifiedhacker.com**. Nikto starts scanning with all the tuning options enabled. The **-h** specifies the target host, and **-x** specifies the reverse tuning options. The scan takes approximately ten minutes to complete. The result appears, displaying various information such as the server’s name, IP address, target port, retrieved files, and vulnerability details of the target website.    7. Execute the command **nikto –h** [**www.certifiedhacker.com**](http://www.certifiedhacker.com) **–Cgidirs all**. The **-Cgidirs** scans the specified CGI directories; users can use filters such as **all** or **none** to scan all CGI directories or none.    8. The target website has no CGI directory; therefore, the same result as the previous scan was obtained. Try this command on another website to obtain information about CGI directories.    9. Type **nikto -h** [**www.certifiedhacker.com**](http://www.certifiedhacker.com) **-o Nikto\_Scan\_Reults –F txt**. The **-h** specifies the target, **-o** specifies the name of the output file, and **-F** specifies the file format. **Nikto\_Scan \_Results** is the file name.    10. Execute the command **pluma Nikto\_Scan\_Results** to open the created file in a text editor window. The file appears to display the scanned results. It concludes the demonstration of checking vulnerabilities in the target website using Nikto. |