Stage 2

Overview :-

Nessus is a powerful and widely respected vulnerability scanning and assessment tool that plays a pivotal role in enhancing the security of networks, systems, and applications. Its primary mission is to assist organizations in proactively identifying and addressing security vulnerabilities. Nessus achieves this through a comprehensive set of features and capabilities.

One of its standout attributes is its ability to conduct exhaustive scans of networks, systems, and web applications, uncovering a wide spectrum of vulnerabilities, ranging from misconfigurations to missing patches and other common security weaknesses. This breadth of coverage is made possible by Nessus's plugin-based architecture, which supports an extensive library of plugins. This versatility enables users to tailor scans to their specific needs, making it a flexible tool suitable for a diverse array of organizations.

In addition to vulnerability assessment, Nessus offers the capability to evaluate systems and applications for compliance with established security standards and regulations. Its scanning policies can be customized, scan schedules can be configured, and scan parameters can be fine-tuned to match particular requirements. The resulting detailed reports, highlighting vulnerabilities, their severity, and recommended remediation steps, are invaluable resources for IT administrators and security professionals seeking to bolster their defenses.

Nessus's scalability is another distinguishing feature, making it accessible to organizations of varying sizes. Whether deployed in small or large environments, Nessus is equipped to efficiently identify and report on vulnerabilities. Furthermore, its integration capabilities allow it to seamlessly work in conjunction with other security tools and management systems, enabling users to create a holistic security ecosystem.

While Nessus's capabilities are remarkable, it is imperative that users exercise caution and adhere to ethical standards. Unauthorized scanning can disrupt systems and potentially lead to legal and ethical violations. Therefore, Nessus is most effective and responsible when used with proper permissions, making it an indispensable tool for security professionals in safeguarding digital assets and fortifying the defenses of modern organizations.

Target website :

Testfire.net

Target ip address:

65.61.137.117

List of vulnerability □

s.no	Vulnerability name	Severity	plugins
1.	- CGI Generic XSS (comprehensive test)	MEDIUM	47831

2.	Web Application Potentially Vulnerable to Clickjacking	MEDIUM	85582
3.	Web Server Allows Password Auto-Completion	LOW	42057
4.	Web Server Transmits Cleartext Credentials	LOW	26194
5.	Apache Tomcat Detection	INFO	39446
6.	CGI Generic Injectable Parameter	INFO	47830
7.	CGI Generic Tests HTTP Errors	INFO	40406
8.	CGI Generic Tests Load Estimation (all tests)	INFO	33817 –
9.			

10.	CGI Generic Tests Timeout	INFO	39470
11.	External URLs	INFO	49704
12.	HSTS Missing From HTTPS Server	INFO	84502
13.	HTTP Cookie 'secure' Property Transport Mismatch	INFO	69826 –
14.	HTTP Methods Allowed (per directory)	INFO	43111
15.	HTTP Server Type and Version	INFO	10107 –

16.	HyperText Transfer Protocol (HTTP) Information	INFO	24260
17.	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	INFO	50344
18.	Missing or Permissive X-Frame-Options HTTP Response Header	INFO	50345
19.	Nessus SYN scanner	INFO	11219
20.	Nessus Scan Information	INFO	19506
21.	Web Application Cookies Not Marked Secure		85602
	Web Application		

22. 23.	Sitemap Web mirroring		91815 10662

REPORT:-

Vulnerability Name:-

severity : -

Plugin:-

Port :-

Description:-

solution:-

Business Impact::-