Clickjacking Vulnerability Assessment Report

This Proof of Concept (PoC) documents the process and results of a vulnerability assessment conducted using a vulnerability scanning tool (OpenVAS/Nessus Essentials). The scan identified a critical vulnerability: **Clickjacking**. This report details the methodology, findings, impact, and recommendations for mitigation.

Methodology

1. Installation: Installed Nessus Essentials/OpenVAS.
2. Target Setup: Configured the scan target as the local machine IP/localhost.
3. Scan Execution: Performed a full vulnerability scan.
4. Analysis: Waited for scan completion (30-60 mins).
5. Review: Analyzed the generated report.

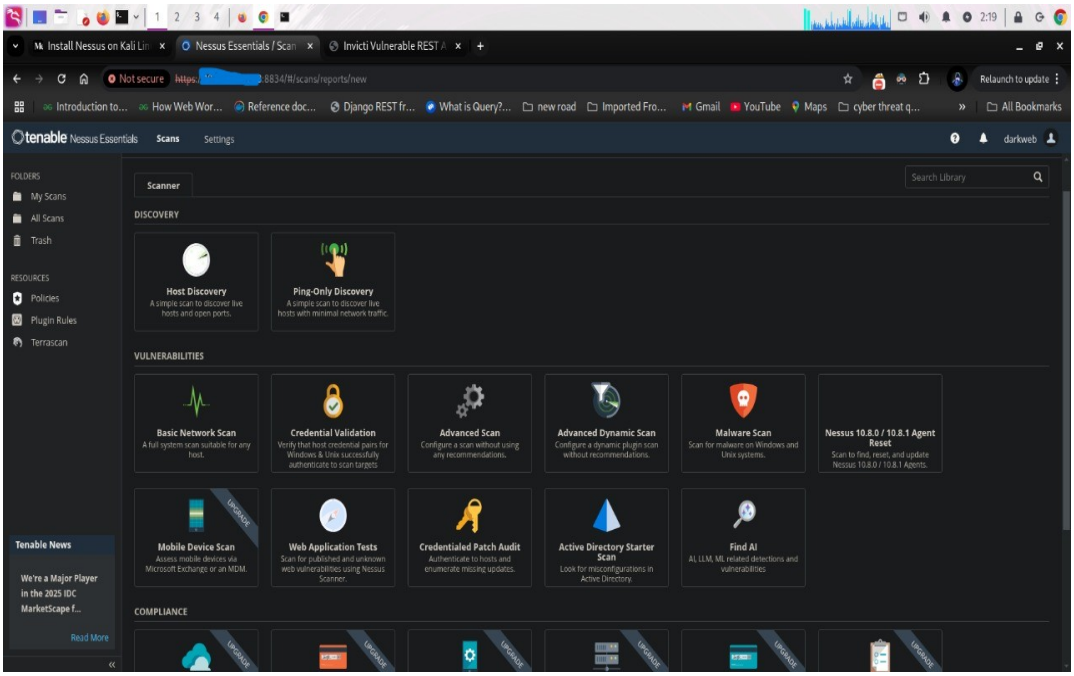
Vulnerability Details

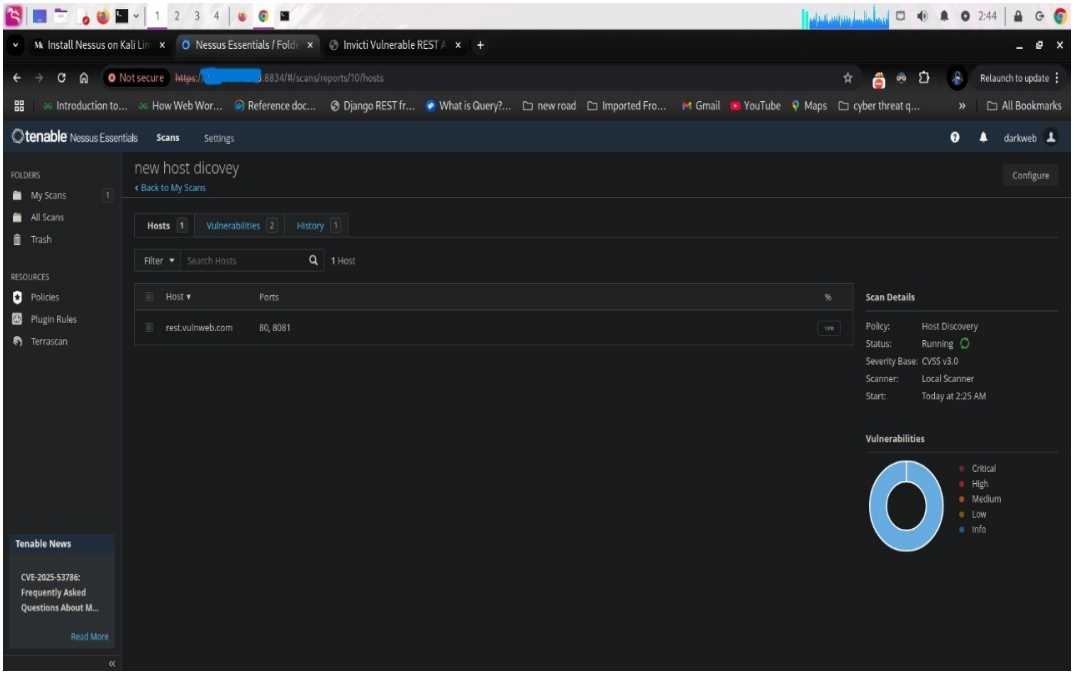
Vulnerability Name: Clickjacking
Severity: High
Description: Clickjacking is a malicious technique of tricking a web user into clicking on something different from what the user perceives, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.
Impact: Attackers can overlay transparent or opaque layers to intercept user clicks meant for trusted web applications. This could lead to unauthorized actions, data theft, or privilege escalation.

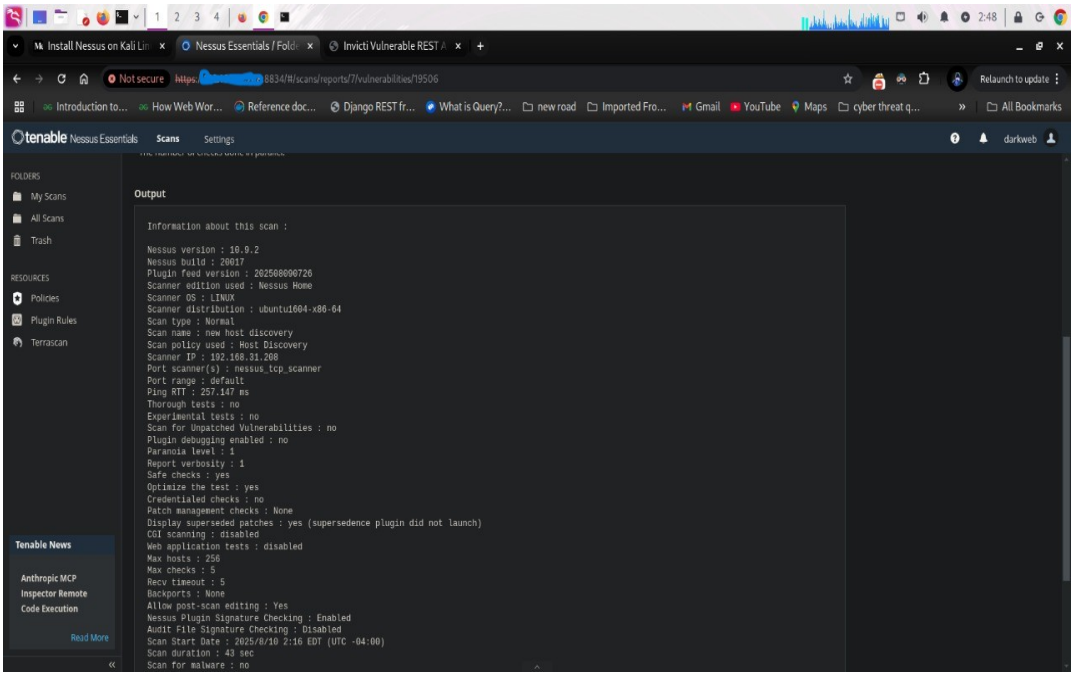
Recommendations

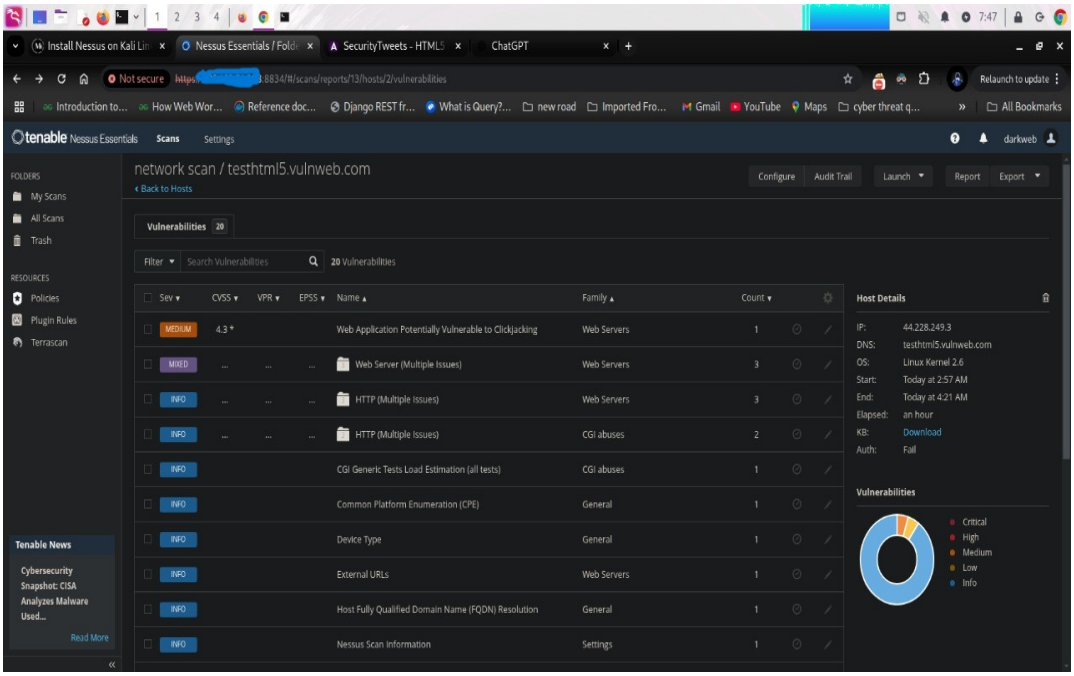
Mitigation:
1. Implement the X-Frame-Options HTTP header with the value "DENY" or "SAMEORIGIN".
2. Use Content Security Policy (CSP) frame-ancestors directive to control allowed domains.
3. Regularly perform security testing to ensure the protection is in place.

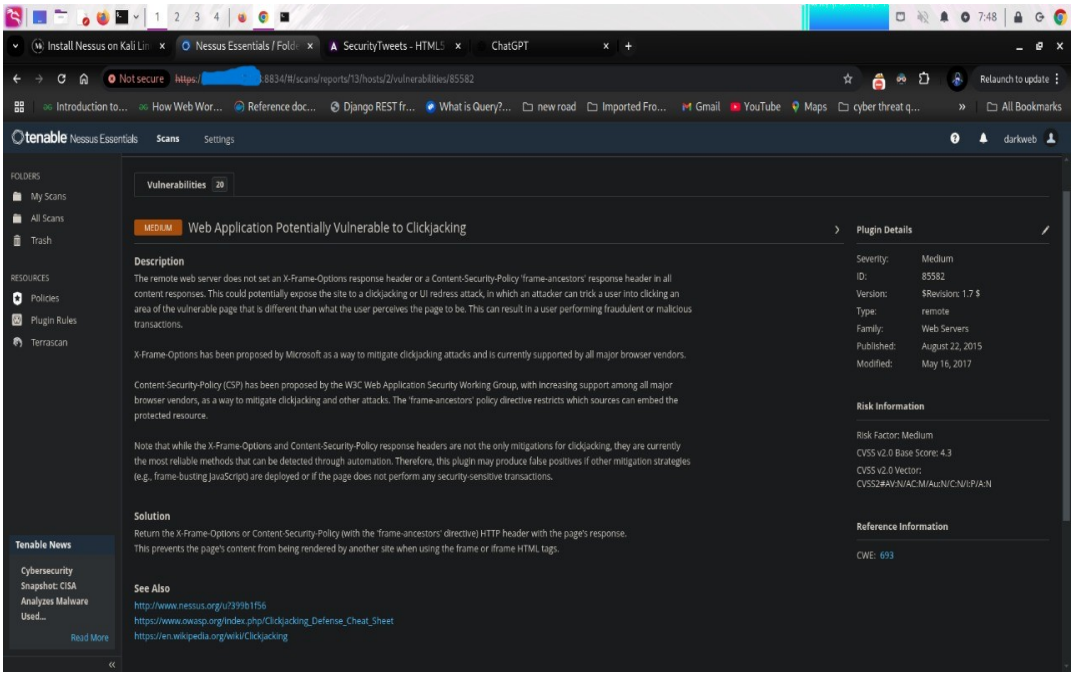
Scan Evidence

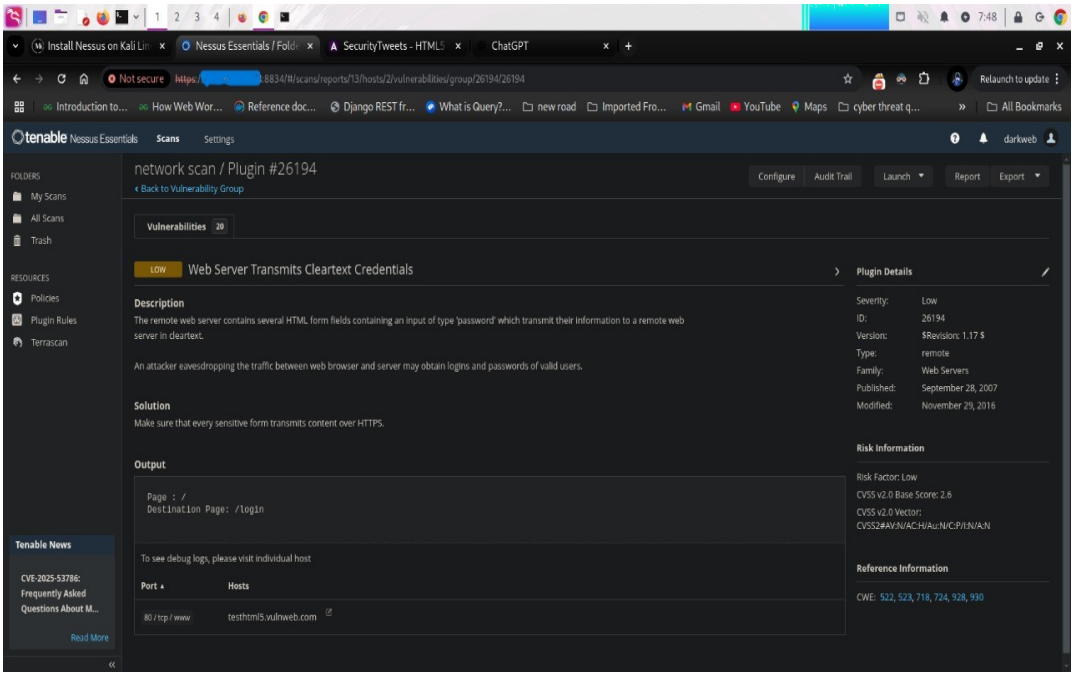

Install Nessus on Kali Lin
Nessus Essentials / Scan
Invicti Vulnerable REST A
Not secure
Relaunch to update
Introduction to...
How Web Wor...
Reference doc...
Django REST fr...
What is Query?...
new road
Imported Fro...
Gmail
YouTube
Maps
cyber threat q...
All Bookmarks
tenable Nessus Essentials
Scans
Settings
darkweb
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Scanner
Search Library
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
Ping-Only Discovery
A simple scan to discover live hosts with minimal network traffic.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Credential Validation
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
Nessus 10.8.0 / 10.8.1 Agent Reset
Scan to find, reset, and update Nessus 10.8.0 / 10.8.1 Agents.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Active Directory Starter Scan
Look for misconfigurations in Active Directory.
Find AI
AI, LLM, ML related detections and vulnerabilities
UPGRADE
Tenable News
We're a Major Player in the 2025 IDC MarketScape f...
Read More
COMPLIANCE


Install Nessus on Kali Lin
Nessus Essentials / Fold
Invicti Vulnerable REST A
Not secure
Relaunch to update
Introduction to...
How Web Wor...
Reference doc...
Django REST fr...
What is Query?...
new road
Imported Fro...
Gmail
YouTube
Maps
cyber threat q...
All Bookmarks
tenable Nessus Essentials
Scans
Settings
darkweb
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
new host dicovey
Back to My Scans
Configure
Hosts 1
Vulnerabilities 2
History 1
Filter
Search Hosts
1 Host
Host
Ports
%
rest.vulnweb.com
80, 8081
Scan Details
Policy: Host Discovery
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 2:25 AM
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
CVE-2025-53786: Frequently Asked Questions About M...
Read More


Output
Information about this scan :
Nessus version : 10.9.2
Nessus build : 20017
Plugin feed version : 202508090726
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : new host discovery
Scan policy used : Host Discovery
Scanner IP : 192.168.31.208
Port scanner(s) : nessus_tcp_scanner
Port range : default
Ping RTT : 257.147 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/8/10 2:16 EDT (UTC -04:00)
Scan duration : 43 sec
Scan for malware : no


network scan / testhtml5.vulnweb.com
Back to Hosts
Vulnerabilities 20
20 Vulnerabilities
Host Details
IP: 44.228.249.3
DNS: testhtml5.vulnweb.com
OS: Linux Kernel 2.6
Start: Today at 2:57 AM
End: Today at 4:21 AM
Elapsed: an hour
KB: Download
Auth: Fail
Vulnerabilities
Critical
High
Medium
Low
Info


Install Nessus on Kali Lin
Nessus Essentials / Folde
SecurityTweets - HTML5
ChatGPT
Not secure
https:/ :8834/#/scans/reports/13/hosts/2/vulnerabilities/85582
Relaunch to update
Introduction to...
How Web Wor...
Reference doc...
Django REST fr...
What is Query?...
new road
Imported Fro...
Gmail
YouTube
Maps
cyber threat q...
All Bookmarks
tenable Nessus Essentials
Scans
Settings
darkweb
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: CISA Analyzes Malware Used...
Read More
Vulnerabilities 20
MEDIUM
Web Application Potentially Vulnerable to Clickjacking
Description
The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.
X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.
Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.
Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.
Solution
Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.
See Also
http://www.nessus.org/u?399b1f56
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet
https://en.wikipedia.org/wiki/Clickjacking
Plugin Details
Severity: Medium
ID: 85582
Version: $Revision: 1.7 $
Type: remote
Family: Web Servers
Published: August 22, 2015
Modified: May 16, 2017
Risk Information
Risk Factor: Medium
CVSS v2.0 Base Score: 4.3
CVSS v2.0 Vector:
CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N
Reference Information
CWE: 693


Install Nessus on Kali Lin
Nessus Essentials / Folde
SecurityTweets - HTML5
ChatGPT
Not secure
https:/ :8834/#/scans/reports/13/hosts/2/vulnerabilities/group/26194/26194
Relaunch to update
Introduction to...
How Web Wor...
Reference doc...
Django REST fr...
What is Query?...
new road
Imported Fro...
Gmail
YouTube
Maps
cyber threat q...
All Bookmarks
tenable Nessus Essentials
Scans
Settings
darkweb
network scan / Plugin #26194
‹ Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
CVE-2025-53786: Frequently Asked Questions About M...
Read More
Vulnerabilities 20
LOW
Web Server Transmits Cleartext Credentials
Description
The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.
An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.
Solution
Make sure that every sensitive form transmits content over HTTPS.
Output
Page : /
Destination Page: /login
To see debug logs, please visit individual host
Port ▲
Hosts
80 / tcp / www
testhtml5.vulnweb.com
Plugin Details
Severity: Low
ID: 26194
Version: $Revision: 1.17 $
Type: remote
Family: Web Servers
Published: September 28, 2007
Modified: November 29, 2016
Risk Information
Risk Factor: Low
CVSS v2.0 Base Score: 2.6
CVSS v2.0 Vector:
CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N
Reference Information
CWE: 522, 523, 718, 724, 928, 930