**REPORT OF Kongu.ac.in**

[ Checking Available Security Scanning Tools Phase... Initiated. ]

Some of these tools ['golismero'] are unavailable or will be skipped. RapidScan will still perform the rest of the tests. Install these tools to fully utilize the functionality of RapidScan.

[ Checking Available Security Scanning Tools Phase... Completed. ]

[ Preliminary Scan Phase Initiated... Loaded 80 vulnerability checks. ]

[● < 45s] Deploying 1/80 | Wafw00f - Checks for Application Firewalls.

Scan Completed in 23s

[● < 35s] Deploying 2/80 | Nmap [OpenSSL CCS Injection] - Checks only for CCS Injection.

Scan Completed in 7s

[● < 35s] Deploying 3/80 | Nikto - Checks for HTTP Options on the Domain.

Scan Completed in 3m 48s

[● < 35s] Deploying 4/80 | Nikto - Checks for Apache Expect XSS Header.

Scan Completed in 2m 14s

[● < 30s] Deploying 5/80 | ASP.Net Misconfiguration - Checks for ASP.Net Misconfiguration.

Scan Completed in 3s

[● < 9m] Deploying 6/80 | Uniscan - Stress Tests the Domain.

Scan Completed in 10s

[● < 75m] Deploying 7/80 | Fierce Subdomains Bruter - Brute Forces Subdomain Discovery.

Scan Completed in 4m 50s

Vulnerability Threat Level

medium Found Subdomains with Fierce.

Vulnerability Definition

Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances for the attacker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.

Vulnerability Remediation

It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.

[● < 15s] Deploying 8/80 | Nmap [FTP] - Checks if FTP service is running.

Scan Completed in 2s

Vulnerability Threat Level

critical FTP Service Detected.

Vulnerability Definition

This protocol does not support secure communication and there are likely high chances for the attacker to eavesdrop the communication. Also, many FTP programs have exploits available in the web such that an attacker can directly crash the application or either get a SHELL access to that target.

Vulnerability Remediation

Proper suggested fix is use an SSH protocol instead of FTP. It supports secure communication and chances for MiTM attacks are quite rare.

[● < 35s] Deploying 9/80 | Nikto - Checks for MS10-070 Vulnerability.

Scan Completed in 1m 31s

[● < 30s] Deploying 10/80 | WordPress Checker - Checks for WordPress Installation.

Scan Completed in 3s

[● < 45s] Deploying 11/80 | Golismero - SQLMap [Retrieves only the DB Banner]

Scanning Tool Unavailable. Skipping Test...

[● < 15s] Deploying 12/80 | Nmap - Checks for MySQL DB

Scan Completed in 2s

Vulnerability Threat Level

low MySQL DB Service Detected.

Vulnerability Definition

Since the attacker has knowledge about the particular type of backend the target is running, they will be able to launch a targetted exploit for the particular version. They may also try to authenticate with default credentials to get themselves through.

Vulnerability Remediation

Timely security patches for the backend has to be installed. Default credentials has to be changed. If possible, the banner information can be changed to mislead the attacker. The following resource gives more information on how to secure your backend. http://kb.bodhost.com/secure-database-server/

[● < 35s] Deploying 13/80 | Nikto - Performs SSL Checks.

Scan Completed in 1m 58s

[● < 35s] Deploying 14/80 | Nikto - Enumerates CGI Directories.

Scan Completed in 2m 6s

[● < 5m] Deploying 15/80 | Wapiti - Checks for SQLi, RCE, XSS and Other Vulnerabilities

Scan Completed in 8s

[● < 15s] Deploying 16/80 | Nmap - Checks for Remote Desktop Service over UDP

Scan Completed in 1s

[● < 2m] Deploying 17/80 | Uniscan - Brutes for Filenames on the Domain.

Scan Completed in 6s

[● < 30s] Deploying 18/80 | Drupal Checker - Checks for Drupal Installation.

Scan Completed in 4s

[● < 30s] Deploying 19/80 | Joomla Checker - Checks for Joomla Installation.

Scan Completed in 5s

[● < 40s] Deploying 20/80 | Nmap - Checks for IIS WebDAV

Scan Completed in 7s

[● < 20s] Deploying 21/80 | Nmap [XSS Filter Check] - Checks if XSS Protection Header is present.

Scan Completed in 7s

[● < 15m] Deploying 22/80 | AMass - Brutes Domain for Subdomains

Scan Interrupted in 5m 23s

Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.

[● < 3m] Deploying 23/80 | The Harvester - Scans for emails using Google's passive search.

Scan Completed in 13s

[● < 40s] Deploying 24/80 | SSLyze - Checks only for Heartbleed Vulnerability.

Scan Completed in 20s

[● < 35m] Deploying 25/80 | DirB - Brutes the target for Open Directories.

Scan Interrupted in 54s

Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.

[● > 75m] Deploying 26/80 | Nmap - Performs a Full UDP Port Scan

Scan Completed in 1s

[● < 35s] Deploying 27/80 | Nikto - Checks for any interesting files on the Domain.

Scan Completed in 14m 28s

Vulnerability Threat Level

medium Interesting Files Detected.

Vulnerability Definition

Attackers may find considerable amount of information from these files. There are even chances attackers may get access to critical information from these files.

Vulnerability Remediation

It is recommended to block or restrict access to these files unless necessary.

[● < 3m] Deploying 28/80 | WhatWeb - Checks for X-XSS Protection Header

Scan Completed in 25s

Vulnerability Threat Level

medium X-XSS Protection is not Present

Vulnerability Definition

As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.

Vulnerability Remediation

Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.

[● < 35s] Deploying 29/80 | Nikto - Checks if Server is Outdated.

Scan Completed in 1m 44s

[● < 2m] Deploying 30/80 | Nmap - Fast Scan [Only Few Port Checks]

Scan Completed in 49s

Vulnerability Threat Level

low Some ports are open. Perform a full-scan manually.

Vulnerability Definition

Open Ports give attackers a hint to exploit the services. Attackers try to retrieve banner information through the ports and understand what type of service the host is running

Vulnerability Remediation

It is recommended to close the ports of unused services and use a firewall to filter the ports wherever necessary. This resource may give more insights. https://security.stackexchange.com/a/145781/6137

[● < 35s] Deploying 31/80 | Nmap [LOGJAM] - Checks for LOGJAM Vulnerability.

Scan Completed in 17s

[● < 30s] Deploying 32/80 | Nmap [FREAK] - Checks only for FREAK Vulnerability.

Scan Completed in 15s

[● < 35s] Deploying 33/80 | Nikto - Checks for Injectable Paths.

Scan Completed in 2m 9s

[● < 20s] Deploying 34/80 | Checks for SMB Service over UDP

Scan Completed in 5s

[● < 25s] Deploying 35/80 | SSLyze - Checks for Secure Renegotiation Support and Client Renegotiation.

Scan Completed in 10s

Vulnerability Threat Level

medium Secure Client Initiated Renegotiation is supported.

Vulnerability Definition

Otherwise termed as Plain-Text Injection attack, which allows MiTM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context.

Vulnerability Remediation

Detailed steps of remediation can be found from these resources. https://securingtomorrow.mcafee.com/technical-how-to/tips-securing-ssl-renegotiation/ https://www.digicert.com/news/2011-06-03-ssl-renego/

[● < 30m] Deploying 36/80 | DNSMap - Brutes Subdomains.

Scan Interrupted in 2m 3s

Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.

[● < 15s] Deploying 37/80 | Nmap - Checks for Remote Desktop Service over TCP

Scan Completed in 3s

[● < 40s] Deploying 38/80 | Uniscan - Checks for robots.txt & sitemap.xml

Scan Completed in 5s

[● < 30s] Deploying 39/80 | WebDAV - Checks if WEBDAV enabled on Home directory.

Scan Completed in 9s

[● < 30s] Deploying 40/80 | Nmap - Checks for SNMP Service

Scan Completed in 1s

[● < 15s] Deploying 41/80 | Nmap - Checks for MS-SQL Server DB

Scan Completed in 4s

[● < 25s] Deploying 42/80 | SSLyze - Checks for OCSP Stapling.

Scan Completed in 10s

[● < 40s] Deploying 43/80 | Golismero - Checks only for Heartbleed Vulnerability.

Scanning Tool Unavailable. Skipping Test...

[● < 15s] Deploying 44/80 | Golismero - Does a fingerprint on the Domain.

Scanning Tool Unavailable. Skipping Test...

[● < 4m] Deploying 45/80 | XSSer - Checks for Cross-Site Scripting [XSS] Attacks.

Scan Completed in 2m 11s

Vulnerability Threat Level

critical XSSer found XSS vulnerabilities.

Vulnerability Definition

An attacker will be able to steal cookies, deface web application or redirect to any third party address that can serve malware.

Vulnerability Remediation

Input validation and Output Sanitization can completely prevent Cross Site Scripting (XSS) attacks. XSS attacks can be mitigated in future by properly following a secure coding methodology. The following comprehensive resource provides detailed information on fixing this vulnerability. https://www.owasp.org/index.php/XSS\_(Cross\_Site\_Scripting)\_Prevention\_Cheat\_Sheet

[● < 35s] Deploying 46/80 | DMitry - Passively Harvests Subdomains from the Domain.

Scan Completed in 23s

Vulnerability Threat Level

medium Subdomains discovered with DMitry.

Vulnerability Definition

Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances for the attacker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.

Vulnerability Remediation

It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.

[● < 4m] Deploying 47/80 | LBD - Checks for DNS/HTTP Load Balancers.

Scan Completed in 3m 16s

Vulnerability Threat Level

low No DNS/HTTP based Load Balancers Found.

Vulnerability Definition

This has nothing to do with security risks, however attackers may use this unavailability of load balancers as an advantage to leverage a denial of service attack on certain services or on the whole application itself.

Vulnerability Remediation

Load-Balancers are highly encouraged for any web application. They improve performance times as well as data availability on during times of server outage. To know more information on load balancers and setup, check this resource. https://www.digitalocean.com/community/tutorials/what-is-load-balancing

[● < 30s] Deploying 48/80 | Nmap [Heartbleed] - Checks only for Heartbleed Vulnerability.

Scan Completed in 6s

[● < 5m] Deploying 49/80 | Uniscan - Brutes Directories on the Domain.

Scan Completed in 6s

[● < 35s] Deploying 50/80 | Nikto - Checks the Domain Headers.

Scan Completed in 2m 13s

Vulnerability Threat Level

medium Some vulnerable headers exposed.

Vulnerability Definition

Attackers try to learn more about the target from the amount of information exposed in the headers. An attacker may know what type of tech stack a web application is emphasizing and many other information.

Vulnerability Remediation

Banner Grabbing should be restricted and access to the services from outside would should be made minimum.

[● < 30s] Deploying 51/80 | DMitry - Passively Harvests Emails from the Domain.

Scan Completed in 5s

[● < 35s] Deploying 52/80 | Nikto - Brutes Subdomains.

Scan Completed in 2m 11s

[● > 50m] Deploying 53/80 | Nmap - Performs a Full TCP Port Scan

Scan Interrupted in 44m 1s

Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.

[● < 15s] Deploying 54/80 | Nmap - Checks for ORACLE DB

Scan Completed in 7s

[● < 35s] Deploying 55/80 | Nikto - Checks for Shellshock Bug.

Scan Completed in 11m 51s

[● < 35s] Deploying 56/80 | DNSWalk - Attempts Zone Transfer.

Scan Completed in 3s

[● < 35s] Deploying 57/80 | Nmap [POODLE] - Checks only for Poodle Vulnerability.

Scan Completed in 8s

[● < 20s] Deploying 58/80 | Nmap [STUXNET] - Checks if the host is affected by STUXNET Worm.

Scan Completed in 4s

[● < 30s] Deploying 59/80 | SSLyze - Checks for ZLib Deflate Compression.

Scan Completed in 9s

[● < 15s] Deploying 60/80 | Nmap [TELNET] - Checks if TELNET service is running.

Scan Completed in 4s

[● < 40s] Deploying 61/80 | Golismero - BruteForces for certain directories on the Domain.

Scanning Tool Unavailable. Skipping Test...

[● < 4m] Deploying 62/80 | Golismero Nikto Scans - Uses Nikto Plugin to detect vulnerabilities.

Scanning Tool Unavailable. Skipping Test...

[● < 9m] Deploying 63/80 | Uniscan - Checks for XSS, SQLi, BSQLi & Other Checks.

Scan Completed in 6s

[● < 20s] Deploying 64/80 | Checks for SMB Service over TCP

Scan Completed in 4s

[● < 30s] Deploying 65/80 | Golismero Zone Transfer - Attempts Zone Transfer.

Scanning Tool Unavailable. Skipping Test...

[● < 45s] Deploying 66/80 | DNSEnum - Attempts Zone Transfer.

Scan Interrupted in 20m 45s

Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.

[● < 20s] Deploying 67/80 | DNSRecon - Attempts Multiple Zone Transfers on Nameservers.

Scan Interrupted in 19s

Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.

[● < 30s] Deploying 68/80 | Checks for ASP.net Elmah Logger

Scan Completed in 6s

[● < 45s] Deploying 69/80 | Golismero - Checks if the domain is spoofed or hijacked.

Scanning Tool Unavailable. Skipping Test...

[● < 30s] Deploying 70/80 | SSLyze - Checks for Session Resumption Support with [Session IDs/TLS Tickets].

Scan Completed in 15s

[● < 45m] Deploying 71/80 | Nmap [Slowloris DoS] - Checks for Slowloris Denial of Service Vulnerability.

Scan Interrupted in 7m 37s

Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.

[● < 45s] Deploying 72/80 | Golismero - BruteForces for certain files on the Domain.

Scanning Tool Unavailable. Skipping Test...

[● < 35s] Deploying 73/80 | Nikto - Checks for Internal IP Leak.

Scan Completed in 1m 51s

[● < 30m] Deploying 74/80 | Golismero Subdomains Bruter - Brute Forces Subdomain Discovery.

Scanning Tool Unavailable. Skipping Test...

[● < 35s] Deploying 75/80 | Nikto - Checks for Server Issues.

Scan Completed in 2m 1s

[● < 15s] Deploying 76/80 | Host - Checks for existence of IPV6 address.

Scan Completed in 2s

Vulnerability Threat Level

info Does not have an IPv6 Address. It is good to have one.

Vulnerability Definition

Not a vulnerability, just an informational alert. The host does not have IPv6 support. IPv6 provides more security as IPSec (responsible for CIA - Confidentiality, Integrity and Availablity) is incorporated into this model. So it is good to have IPv6 Support.

Vulnerability Remediation

It is recommended to implement IPv6. More information on how to implement IPv6 can be found from this resource. https://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/IPv6-Implementation\_CS.html

[● < 45s] Deploying 77/80 | Golismero SSL Scans - Performs SSL related Scans.

Scanning Tool Unavailable. Skipping Test...

[● < 35s] Deploying 78/80 | Nikto - Checks for HTTP PUT DEL.

Scan Completed in 1m 42s

[● < 8m] Deploying 79/80 | Uniscan - Checks for LFI, RFI and RCE.

Scan Completed in 7s

[● < 25s] Deploying 80/80 | WHOis - Checks for Administrator's Contact Information.

Scan Completed in 1s

Vulnerability Threat Level

info Whois Information Publicly Available.

Vulnerability Definition

The email address of the administrator and other information (address, phone, etc) is available publicly. An attacker may use these information to leverage an attack. This may not be used to carry out a direct attack as this is not a vulnerability. However, an attacker makes use of these data to build information about the target.

Vulnerability Remediation

Some administrators intentionally would have made this information public, in this case it can be ignored. If not, it is recommended to mask the information. This resource provides information on this fix. http://www.name.com/blog/how-tos/tutorial-2/2013/06/protect-your-personal-information-with-whois-privacy/

[ Preliminary Scan Phase Completed. ]

[ Report Generation Phase Initiated. ]

Complete Vulnerability Report for kongu.ac.in named rs.vul.kongu.ac.in.2024-09-16 is available under the same directory RapidScan resides.

Total Number of Vulnerability Checks : 80

Total Number of Vulnerability Checks Skipped: 17

Total Number of Vulnerabilities Detected : 13

Total Time Elapsed for the Scan : 2h 29m 4s