**Report Of ksrce.ac.in**

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

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

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

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

[● < 20s] Deploying 1/80 | DNSRecon - Attempts Multiple Zone Transfers on Nameservers.

Scan Completed in 18s

[● < 40s] Deploying 2/80 | Golismero - Checks only for Heartbleed Vulnerability.

Scanning Tool Unavailable. Skipping Test...

[● < 75m] Deploying 3/80 | Fierce Subdomains Bruter - Brute Forces Subdomain Discovery.

Scan Completed in 4m 27s

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.

[● < 40s] Deploying 4/80 | SSLyze - Checks only for Heartbleed Vulnerability.

Scan Completed in 12s

[● < 15s] Deploying 5/80 | Nmap - Checks for Remote Desktop Service over UDP

Scan Completed in 1s

[● < 35s] Deploying 6/80 | DMitry - Passively Harvests Subdomains from the Domain.

Scan Completed in 44s

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.

[● < 30s] Deploying 7/80 | WordPress Checker - Checks for WordPress Installation.

Scan Completed in 2s

[● < 20s] Deploying 8/80 | Checks for SMB Service over TCP

Scan Completed in 5s

[● < 30s] Deploying 9/80 | SSLyze - Checks for Session Resumption Support with [Session IDs/TLS Tickets].

Scan Completed in 12s

[● < 9m] Deploying 10/80 | Uniscan - Checks for XSS, SQLi, BSQLi & Other Checks.

Scan Completed in 8s

[● < 25s] Deploying 11/80 | WHOis - Checks for Administrator's Contact Information.

Scan Completed in 2s

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/

[● < 35s] Deploying 12/80 | Nmap [POODLE] - Checks only for Poodle Vulnerability.

Scan Completed in 6s

[● < 35s] Deploying 13/80 | DNSWalk - Attempts Zone Transfer.

Scan Completed in 4s

[● < 25s] Deploying 14/80 | SSLyze - Checks for Secure Renegotiation Support and Client Renegotiation.

Scan Completed in 8s

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/

[● < 30s] Deploying 15/80 | Golismero Zone Transfer - Attempts Zone Transfer.

Scanning Tool Unavailable. Skipping Test...

[● < 5m] Deploying 16/80 | Uniscan - Brutes Directories on the Domain.

Scan Completed in 7s

[● < 15s] Deploying 17/80 | Nmap - Checks for Remote Desktop Service over TCP

Scan Completed in 4s

[● < 35m] Deploying 18/80 | DirB - Brutes the target for Open Directories.

Busybees received a series of Ctrl+C hits. Quitting...

Scan Completed in 10m 38s

[● < 20s] Deploying 19/80 | Nmap [STUXNET] - Checks if the host is affected by STUXNET Worm.

Scan Completed in 24s

[● < 30s] Deploying 20/80 | Drupal Checker - Checks for Drupal Installation.

Scan Completed in 11s

[● < 45s] Deploying 21/80 | DNSEnum - Attempts Zone Transfer.

Busybees received a series of Ctrl+C hits. Quitting...

Scan Interrupted in 10m 56s

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

[● < 40s] Deploying 22/80 | Nmap - Checks for IIS WebDAV

Scan Completed in 7s

[● < 30m] Deploying 23/80 | Golismero Subdomains Bruter - Brute Forces Subdomain Discovery.

Scanning Tool Unavailable. Skipping Test...

[● < 45s] Deploying 24/80 | Golismero - BruteForces for certain files on the Domain.

Scanning Tool Unavailable. Skipping Test...

[● < 15s] Deploying 25/80 | Host - Checks for existence of IPV6 address.

Scan Completed in 4s

[● < 35s] Deploying 26/80 | Nikto - Checks for HTTP PUT DEL.

Scan Completed in 50s

[● < 15s] Deploying 27/80 | Nmap [FTP] - Checks if FTP service is running.

Scan Completed in 4s

[● < 15s] Deploying 28/80 | Nmap - Checks for MySQL DB

Scan Completed in 5s

[● < 30s] Deploying 29/80 | Nmap - Checks for SNMP Service

Scan Completed in 1s

[● < 2m] Deploying 30/80 | Uniscan - Brutes for Filenames on the Domain.

Scan Completed in 13s

[● < 3m] Deploying 31/80 | The Harvester - Scans for emails using Google's passive search.

Busybees received a series of Ctrl+C hits. Quitting...

Scan Completed in 34s

[● < 40s] Deploying 32/80 | Golismero - BruteForces for certain directories on the Domain.

Scanning Tool Unavailable. Skipping Test...

[● < 35s] Deploying 33/80 | Nikto - Checks for MS10-070 Vulnerability.

Scan Completed in 45s

[● < 35s] Deploying 34/80 | Nikto - Checks for HTTP Options on the Domain.

Scan Completed in 46s

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

Busybees received a series of Ctrl+C hits. Quitting...

Scan Completed in 49s

[● < 4m] Deploying 36/80 | LBD - Checks for DNS/HTTP Load Balancers.

Scan Completed in 1m 35s

[● < 30s] Deploying 37/80 | Nmap [Heartbleed] - Checks only for Heartbleed Vulnerability.

Scan Completed in 8s

[● < 30s] Deploying 38/80 | ASP.Net Misconfiguration - Checks for ASP.Net Misconfiguration.

Scan Completed in 3s

[● < 15m] Deploying 39/80 | AMass - Brutes Domain for Subdomains

Busybees received a series of Ctrl+C hits. Quitting...

Scan Interrupted in 2m 12s

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

[● > 75m] Deploying 40/80 | Nmap - Performs a Full UDP Port Scan

Scan Completed in 1s

[● < 15s] Deploying 41/80 | Nmap [TELNET] - Checks if TELNET service is running.

Scan Completed in 6s

[● < 15s] Deploying 42/80 | Nmap - Checks for MS-SQL Server DB

Scan Completed in 4s

[● < 9m] Deploying 43/80 | Uniscan - Stress Tests the Domain.

Busybees received a series of Ctrl+C hits. Quitting...

Scan Completed in 14s

[● < 45s] Deploying 44/80 | Wafw00f - Checks for Application Firewalls.

Scan Completed in 29s

Vulnerability Threat Level

medium No Web Application Firewall Detected

Vulnerability Definition

Without a Web Application Firewall, An attacker may try to inject various attack patterns either manually or using automated scanners. An automated scanner may send hordes of attack vectors and patterns to validate an attack, there are also chances for the application to get DoS`ed (Denial of Service)

Vulnerability Remediation

Web Application Firewalls offer great protection against common web attacks like XSS, SQLi, etc. They also provide an additional line of defense to your security infrastructure. This resource contains information on web application firewalls that could suit your application. https://www.gartner.com/reviews/market/web-application-firewall

[● < 8m] Deploying 45/80 | Uniscan - Checks for LFI, RFI and RCE.

Scan Completed in 6s

[● < 30s] Deploying 46/80 | Nmap [FREAK] - Checks only for FREAK Vulnerability.

Scan Completed in 9s

[● < 35s] Deploying 47/80 | Nikto - Checks for Injectable Paths.

Scan Completed in 47s

[● < 25s] Deploying 48/80 | SSLyze - Checks for OCSP Stapling.

Scan Completed in 14s

[● < 35s] Deploying 49/80 | Nikto - Checks for Apache Expect XSS Header.

Scan Completed in 48s

[● < 4m] Deploying 50/80 | Golismero Nikto Scans - Uses Nikto Plugin to detect vulnerabilities.

Scanning Tool Unavailable. Skipping Test...

[● > 50m] Deploying 51/80 | Nmap - Performs a Full TCP Port Scan

Busybees received a series of Ctrl+C hits. Quitting...

Scan Interrupted in 52s

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

[● < 35s] Deploying 52/80 | Nikto - Checks for any interesting files on the Domain.

Scan Completed in 1m 1s

[● < 3m] Deploying 53/80 | WhatWeb - Checks for X-XSS Protection Header

Busybees received a series of Ctrl+C hits. Quitting...

Scan Interrupted in 40s

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

[● < 20s] Deploying 54/80 | Nmap [XSS Filter Check] - Checks if XSS Protection Header is present.

Scan Completed in 6s

[● < 35s] Deploying 55/80 | Nikto - Brutes Subdomains.

Busybees received a series of Ctrl+C hits. Quitting...

Scan Interrupted in 2m 49s

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

[● < 4m] Deploying 56/80 | XSSer - Checks for Cross-Site Scripting [XSS] Attacks.

Scan Completed in 1m 55s

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

[● < 30s] Deploying 57/80 | WebDAV - Checks if WEBDAV enabled on Home directory.

Scan Completed in 44s

[● < 35s] Deploying 58/80 | Nikto - Performs SSL Checks.

Scan Completed in 28s

[● < 20s] Deploying 59/80 | Checks for SMB Service over UDP

Scan Completed in 23s

[● < 35s] Deploying 60/80 | Nikto - Checks the Domain Headers.

Scan Completed in 30s

[● < 30s] Deploying 61/80 | SSLyze - Checks for ZLib Deflate Compression.

Scan Completed in 37s

[● < 40s] Deploying 62/80 | Uniscan - Checks for robots.txt & sitemap.xml

Scan Completed in 30s

[● < 35s] Deploying 63/80 | Nikto - Checks if Server is Outdated.

Scan Completed in 42s

[● < 15s] Deploying 64/80 | Golismero - Does a fingerprint on the Domain.

Scanning Tool Unavailable. Skipping Test...

[● < 30s] Deploying 65/80 | DMitry - Passively Harvests Emails from the Domain.

GET http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&q=allintext:+%3Ca+href%3Dmailto+ksrce.ac.in&start=0&sa=N&filter=1&num=100 HTTP/1.0

Scan Interrupted in 1m 50s

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

[● < 45s] Deploying 66/80 | Golismero SSL Scans - Performs SSL related Scans.

Scanning Tool Unavailable. Skipping Test...

[● < 35s] Deploying 67/80 | Nmap [OpenSSL CCS Injection] - Checks only for CCS Injection.

Scan Completed in 31s

[● < 2m] Deploying 68/80 | Nmap - Fast Scan [Only Few Port Checks]

Scan Completed in 24s

[● < 35s] Deploying 69/80 | Nikto - Checks for Internal IP Leak.

Scan Completed in 46s

[● < 45s] Deploying 70/80 | Golismero - SQLMap [Retrieves only the DB Banner]

Scanning Tool Unavailable. Skipping Test...

[● < 35s] Deploying 71/80 | Nikto - Enumerates CGI Directories.

Scan Completed in 1m 22s

[● < 45m] Deploying 72/80 | Nmap [Slowloris DoS] - Checks for Slowloris Denial of Service Vulnerability.

Busybees received a series of Ctrl+C hits. Quitting...

Scan Interrupted in 1m 33s

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

[● < 30m] Deploying 73/80 | DNSMap - Brutes Subdomains.

Busybees received a series of Ctrl+C hits. Quitting...

Scan Interrupted in 45s

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

[● < 30s] Deploying 74/80 | Checks for ASP.net Elmah Logger

Scan Completed in 4s

[● < 15s] Deploying 75/80 | Nmap - Checks for ORACLE DB

Scan Completed in 5s

[● < 35s] Deploying 76/80 | Nmap [LOGJAM] - Checks for LOGJAM Vulnerability.

Scan Completed in 15s

[● < 45s] Deploying 77/80 | Golismero - Checks if the domain is spoofed or hijacked.

Scanning Tool Unavailable. Skipping Test...

[● < 35s] Deploying 78/80 | Nikto - Checks for Shellshock Bug.

Busybees received a series of Ctrl+C hits. Quitting...

Busybees received a series of Ctrl+C hits. Quitting...

Scan Interrupted in 56s

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

[● < 30s] Deploying 79/80 | Joomla Checker - Checks for Joomla Installation.

Scan Completed in 4s

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

Busybees received a series of Ctrl+C hits. Quitting...

Scan Completed in 35s

[ Preliminary Scan Phase Completed. ]

[ Report Generation Phase Initiated. ]

Complete Vulnerability Report for ksrce.ac.in named rs.vul.ksrce.ac.in.2024-09-27 is available under the same directory Busybees resides.

Total Number of Vulnerability Checks : 80

Total Number of Vulnerability Checks Skipped: 19

Total Number of Vulnerabilities Detected : 6

Total Time Elapsed for the Scan : 59m 56s

For Debugging Purposes, You can view the complete output generated by all the tools named rs.dbg.ksrce.ac.in.2024-09-27 under the same directory.

[ Report Generation Phase Completed. ]