Our Findings

(The Multi-Tool Web Vulnerability Scanner)

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

wapiti...available.

whatweb...available.

nmap...available.

golismero...available.

host...available.

wget...available.

uniscan...available.

wafw00f...available.

dirb...available.

davtest...available.

theharvester...available.

xsser...available.

dnsrecon...available.

fierce...available.

dnswalk...available.

whois...available.

sslyze...available.

lbd...available.

golismero...available.

dnsenum...available.

dmitry...available.

davtest...available.

nikto...available.

dnsmap...available.

All Scanning Tools are available. All vulnerability checks will be performed by RapidScan.

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

[Preliminary Scan Phase Initiated... Loaded 80.0 vulnerability checks.]

[? < 35s] Deploying 1/80.0 | Nikto - Checks for HTTP Options on the Domain. . ...Completed in 1s

- Some issues found with HTTP Options.

Vulnerability Threat Level: Low

Vulnerability Definition

There are chances for an attacker to manipulate files on the webserver.

Vulnerability Remediation

It is recommended to disable the HTTP PUT and DEL methods incase if you don't use any REST API Services. Following resources helps you how to disable these methods.
http://www.techstacks.com/howto/disable-http-methods-in-tomcat.html
https://docs.oracle.com/cd/E19857-01/820-5627/gghwc/index.html
https://developer.ibm.com/answers/questions/321629/how-to-disable-http-methods-head-put-delete-option/

[? < 35s] Deploying 2/80.0 | Nikto - Brutes Subdomains. . ...Completed in 1s

- Found Subdomains with Nikto.

Vulnerability Threat Level: Medium

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.

[? < 35s] Deploying 3/80.0 | Nikto - Checks the Domain Headers. . ...Completed in 1s

- Some vulnerable headers exposed.

Vulnerability Threat Level: Medium

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.

[? < 45s] Deploying 4/80.0 | Golismero - Checks if the domain is spoofed or hijacked. . ...Completed in 1s

- Domain is spoofed/hijacked.

Vulnerability Threat Level: High

Vulnerability Definition

An attacker can forwarded requests that comes to the legitimate URL or web application to a third party address or to the attacker's location that can serve malware and affect the end user's machine.

Vulnerability Remediation

It is highly recommended to deploy DNSSec on the host target. Full deployment of DNSSEC will ensure the end user is connecting to the actual web site or other service corresponding to a particular domain name. For more information, check this resource. https://www.cloudflare.com/dns/dnssec/how-dnssec-works/

[? < 2m] Deploying 5/80.0 | Nmap - Fast Scan [Only Few Port Checks] . . ...Completed in 1s

[? < 15s] Deploying 6/80.0 | Nmap - Checks for MySQL DB . ...Completed in 1s

[? < 9m] Deploying 7/80.0 | Uniscan - Checks for XSS, SQLi, BSQLi & Other Checks. . ...Completed in 1s

[? < 3m] Deploying 8/80.0 | WhatWeb - Checks for X-XSS Protection Header . ...Completed in 1s

- X-XSS Protection is not Present

Vulnerability Threat Level: Medium

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 9/80.0 | Nmap [POODLE] - Checks only for Poodle Vulnerability. . ...Completed in 1s

[? < 25s] Deploying 10/80.0 | SSLyze - Checks for OCSP Stapling. . ...Completed in 1s

[? < 35s] Deploying 11/80.0 | Nikto - Checks for any interesting files on the Domain. . ...Completed in 1s

- Interesting Files Detected.

Vulnerability Threat Level: Medium

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.

[? < 40s] Deploying 12/80.0 | Nmap - Checks for IIS WebDAV . ...Completed in 1s

[? < 15s] Deploying 13/80.0 | Golismero - Does a fingerprint on the Domain. . ...Completed in 1s

- Found some information through Fingerprinting.

Vulnerability Threat Level: Low

Vulnerability Definition

Attackers always do a fingerprint of any server before they launch an attack. Fingerprinting gives them information about the server type, content- they are serving, last modification times etc, this gives an attacker to learn more information about the target

Vulnerability Remediation

A good practice is to obfuscate the information to outside world. Doing so, the attackers will have tough time understanding the server's tech stack and therefore leverage an attack.

[? < 25s] Deploying 14/80.0 | SSLyze - Checks for Secure Renegotiation Support and Client Renegotiation. . ...Completed in 1s

[? < 15s] Deploying 15/80.0 | Host - Checks for existence of IPV6 address. . ...Completed in 1s

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

Vulnerability Threat Level: Info

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

[? < 40s] Deploying 16/80.0 | Uniscan - Checks for robots.txt & sitemap.xml . ...Completed in 1s

[? < 8m] Deploying 17/80.0 | Uniscan - Checks for LFI, RFI and RCE. . ...Completed in 1s

[? < 45s] Deploying 18/80.0 | Golismero SSL Scans - Performs SSL related Scans. . ...Completed in 1s

[? < 30s] Deploying 19/80.0 | SSLyze - Checks for Session Resumption Support with [Session IDs/TLS Tickets]. . ...Completed in 1s

[? < 4m] Deploying 20/80.0 | Golismero Nikto Scans - Uses Nikto Plugin to detect vulnerabilities. . . ...Completed in 1s

- Golismero Nikto Plugin found vulnerabilities.

Vulnerability Threat Level: Medium

Vulnerability Definition

Particular Scanner found multiple vulnerabilities that an attacker may try to exploit the target.

Vulnerability Remediation

Refer to RS-Vulnerability-Report to view the complete information of the vulnerability, once the scan gets completed.

[? < 35s] Deploying 21/80.0 | Nikto - Enumerates CGI Directories. . ...Completed in 1s

- CGI Directories Enumerated.

Vulnerability Threat Level: Low

Vulnerability Definition

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

Vulnerability Remediation

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

[? < 15s] Deploying 22/80.0 | Nmap - Checks for ORACLE DB . ...Completed in 1s

[? < 30s] Deploying 23/80.0 | SSLyze - Checks for ZLib Deflate Compression. . ...Completed in 1s

[? < 30s] Deploying 24/80.0 | ASP.Net Misconfiguration - Checks for ASP.Net Misconfiguration. . ...Completed in 1s

[? < 30s] Deploying 25/80.0 | Nmap [FREAK] - Checks only for FREAK Vulnerability. . . ...Completed in 1s

[? < 45s] Deploying 26/80.0 | Golismero - SQLMap [Retrieves only the DB Banner] . ...Completed in 1s

- DB Banner retrieved with SQLMap.

Vulnerability Threat Level: Low

Vulnerability Definition

May not be SQLi vulnerable. An attacker will be able to know that the host is using a backend for operation.

Vulnerability Remediation

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

[? < 35s] Deploying 27/80.0 | Nmap [OpenSSL CCS Injection] - Checks only for CCS Injection. . ...Completed in 1s

[? < 30m] Deploying 28/80.0 | DNSMap - Brutes Subdomains. . ...Completed in 1s

[? < 35s] Deploying 29/80.0 | Nikto - Checks for Internal IP Leak. . ...Completed in 1s

- Webserver leaks Internal IP.

Vulnerability Threat Level: Low

Vulnerability Definition

Gives attacker an idea on how the address scheming is done internally on the organizational network. Discovering the private addresses used within an organization can help attackers in carrying out network-layer attacks aiming to penetrate the organization's internal infrastructure.

Vulnerability Remediation

Restrict the banner information to the outside world from the disclosing service. More information on mitigating this vulnerability can be found here.
https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed

[? < 30s] Deploying 30/80.0 | Joomla Checker - Checks for Joomla Installation. . ...Completed in 1s

[? < 2m] Deploying 31/80.0 | Uniscan - Brutes for Filenames on the Domain. . ...Completed in 1s

[? < 15s] Deploying 32/80.0 | Nmap - Checks for Remote Desktop Service over UDP . ...Completed in 1s

[? < 75m] Deploying 33/80.0 | Fierce Subdomains Bruter - Brute Forces Subdomain Discovery. . . . .Completed in 1s

- Found Subdomains with Fierce.

Vulnerability Threat Level: Medium

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 34/80.0 | Nmap - Checks for Remote Desktop Service over TCP . ...Completed in 1s

[? < 20s] Deploying 35/80.0 | Checks for SMB Service over TCP . ...Completed in 1s

[? < 35s] Deploying 36/80.0 | DMitry - Passively Harvests Subdomains from the Domain. . ...Completed in 1s

- Subdomains discovered with DMitry.

Vulnerability Threat Level: Medium

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.

[? < 35s] Deploying 37/80.0 | Nikto - Checks for MS10-070 Vulnerability. . ...Completed in 1s

- Webserver vulnerable to MS10-070.

Vulnerability Threat Level: High

Vulnerability Definition

An attacker who successfully exploited this vulnerability could read data, such as the view state, which was encrypted by the server. This vulnerability can also be used for data tampering, which, if successfully exploited, could be used to decrypt and tamper with the data encrypted by the server.

Vulnerability Remediation

Microsoft has released a set of patches on their website to mitigate this issue. The information required to fix this vulnerability can be inferred from this resource.
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-070

[? < 30s] Deploying 38/80.0 | Drupal Checker - Checks for Drupal Installation. . . ...Completed in 1s

[? < 5m] Deploying 39/80.0 | Wapiti - Checks for SQLi, RCE, XSS and Other Vulnerabilities . ...Completed in 1s

[? < 30s] Deploying 40/80.0 | Fierce - Attempts Zone Transfer [No Brute Forcing] . . . .Completed in 1s

[? < 15s] Deploying 41/80.0 | Nmap - Checks for MS-SQL Server DB . ...Completed in 1s

[? < 4m] Deploying 42/80.0 | XSSer - Checks for Cross-Site Scripting [XSS] Attacks. . ...Completed in 1s

- XSSer found XSS vulnerabilities.

Vulnerability Threat Level: Critical

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 43/80.0 | Nmap - Checks for SNMP Service . . ...Completed in 1s

[? < 9m] Deploying 44/80.0 | Uniscan - Stress Tests the Domain. . ...Completed in 1s

[? < 35s] Deploying 45/80.0 | Nikto - Checks for Apache Expect XSS Header. . ...Completed in 1s

- Apache Expect XSS Header not present.

Vulnerability Threat Level: Medium

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.

[? < 30s] Deploying 46/80.0 | WebDAV - Checks if WEBDAV enabled on Home directory. . . ...Completed in 1s

[? < 35s] Deploying 47/80.0 | DNSWalk - Attempts Zone Transfer. . ...Completed in 1s

[? < 15s] Deploying 48/80.0 | Nmap [FTP] - Checks if FTP service is running. . ...Completed in 1s

[? < 20s] Deploying 49/80.0 | Nmap [STUXNET] - Checks if the host is affected by STUXNET Worm. . ...Completed in 1s

[? < 30s] Deploying 50/80.0 | DMitry - Passively Harvests Emails from the Domain. . ...Completed in 1s

- Email Addresses discovered with DMitry.

Vulnerability Threat Level: Low

Vulnerability Definition

Chances are very less to compromise a target with email addresses. However, attackers use this as a supporting data to gather information around the target. An attacker may make use of the username on the email address and perform brute-force attacks on not just email servers, but also on other legitimate panels like SSH, CMS, etc with a password list as they have a legitimate name. This is however a shoot in the dark scenario, the attacker may or may not be successful depending on the level of interest

Vulnerability Remediation

Since the chances of exploitation is feeble there is no need to take action. Perfect remediation would be choosing different usernames for different services will be more thoughtful.

[? < 30m] Deploying 51/80.0 | Golismero Subdomains Bruter - Brute Forces Subdomain Discovery. . ...Completed in 1s

[? < 25s] Deploying 52/80.0 | WHOis - Checks for Administrator's Contact Information. . ...Completed in 1s

[? < 35s] Deploying 53/80.0 | Nikto - Checks for Injectable Paths. . ...Completed in 1s

[? > 75m] Deploying 54/80.0 | Nmap - Performs a Full UDP Port Scan . ...Completed in 1s

[? < 4m] Deploying 55/80.0 | LBD - Checks for DNS/HTTP Load Balancers. . ...Completed in 1s

[? < 35s] Deploying 56/80.0 | Nmap [LOGJAM] - Checks for LOGJAM Vulnerability. . . ...Completed in 1s

[? < 35s] Deploying 57/80.0 | Nikto - Checks if Server is Outdated. . ...Completed in 1s

- Webserver is Outdated.

Vulnerability Threat Level: High

Vulnerability Definition

Any outdated web server may contain multiple vulnerabilities as their support would've been ended. An attacker may make use of such an opportunity to leverage attacks.

Vulnerability Remediation

It is highly recommended to upgrade the web server to the available latest version.

[? < 20s] Deploying 58/80.0 | DNSRecon - Attempts Multiple Zone Transfers on Nameservers. . ...Completed in 1s

[? < 3m] Deploying 59/80.0 | The Harvester - Scans for emails using Google's passive search. . ...Completed in 1s

- Email Addresses Found.

Vulnerability Threat Level: Low

Vulnerability Definition

Chances are very less to compromise a target with email addresses. However, attackers use this as a supporting data to gather information around the target. An attacker may make use of the username on the email address and perform brute-force attacks on not just email servers, but also on other legitimate panels like SSH, CMS, etc with a password list as they have a legitimate name. This is however a shoot in the dark scenario, the attacker may or may not be successful depending on the level of interest

Vulnerability Remediation

Since the chances of exploitation is feeble there is no need to take action. Perfect remediation would be choosing different usernames for different services will be more thoughtful.

[? < 20s] Deploying 60/80.0 | Checks for SMB Service over UDP . ...Completed in 1s

[? < 5m] Deploying 61/80.0 | Uniscan - Brutes Directories on the Domain. . ...Completed in 1s

[? > 50m] Deploying 62/80.0 | Nmap - Performs a Full TCP Port Scan . ...Completed in 1s

[? < 35s] Deploying 63/80.0 | Nikto - Checks for Shellshock Bug. . ...Completed in 1s

- Webserver vulnerable to Shellshock Bug.

Vulnerability Threat Level: Critical

Vulnerability Definition

Attackers exploit the vulnerability in BASH to perform remote code execution on the target. An experienced attacker can easily take over the target system and access the internal sources of the machine

Vulnerability Remediation

This vulnerability can be mitigated by patching the version of BASH. The following resource gives an indepth analysis of the vulnerability and how to mitigate it.
https://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability
https://www.digitalocean.com/community/tutorials/how-to-protect-your-server-against-the-shellshock-bash-vulnerability

[? < 35m] Deploying 64/80.0 | DirB - Brutes the target for Open Directories. . ...Completed in 1s

- Open Directories Found with DirB.

Vulnerability Threat Level: Medium

Vulnerability Definition

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

Vulnerability Remediation

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

[? < 45s] Deploying 65/80.0 | Wafw00f - Checks for Application Firewalls. . ...Completed in 1s

[? < 40s] Deploying 66/80.0 | SSLyze - Checks only for Heartbleed Vulnerability. . ...Completed in 1s

[? < 45m] Deploying 67/80.0 | Nmap [Slowloris DoS] - Checks for Slowloris Denial of Service Vulnerability. . . ...Completed in 1s

[? < 30s] Deploying 68/80.0 | Golismero Zone Transfer - Attempts Zone Transfer. . ...Completed in 1s

[? < 35s] Deploying 69/80.0 | Nikto - Checks for HTTP PUT DEL. . ...Completed in 1s

- HTTP PUT DEL Methods Enabled.

Vulnerability Threat Level: Medium

Vulnerability Definition

There are chances for an attacker to manipulate files on the webserver.

Vulnerability Remediation

It is recommended to disable the HTTP PUT and DEL methods incase if you don't use any REST API Services. Following resources helps you how to disable these methods.
http://www.techstacks.com/howto/disable-http-methods-in-tomcat.html
https://docs.oracle.com/cd/E19857-01/820-5627/gghwc/index.html
https://developer.ibm.com/answers/questions/321629/how-to-disable-http-methods-head-put-delete-option/

[? < 30s] Deploying 70/80.0 | WordPress Checker - Checks for WordPress Installation. . . ...Completed in 1s

[? < 45s] Deploying 71/80.0 | DNSEnum - Attempts Zone Transfer. . . ...Completed in 1s

- Zone Transfer Successful using DNSEnum. Reconfigure DNS immediately.

Vulnerability Threat Level: High

Vulnerability Definition

Zone Transfer reveals critical topological information about the target. The attacker will be able to query all records and will have more or less complete knowledge about your host.

Vulnerability Remediation

Good practice is to restrict the Zone Transfer by telling the Master which are the IPs of the slaves that can be given access for the query. This SANS resource provides more information.
https://www.sans.org/reading-room/whitepapers/dns/securing-dns-zone-transfer-868

[? < 45s] Deploying 72/80.0 | Golismero - BruteForces for certain files on the Domain. . . . .Completed in 1s

- Open Files Found with Golismero BruteForce.

Vulnerability Threat Level: Medium

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.

[? < 15s] Deploying 73/80.0 | Nmap [TELNET] - Checks if TELNET service is running. . . . .Completed in 1s

[? < 40s] Deploying 74/80.0 | Golismero - BruteForces for certain directories on the Domain. . . ...Completed in 1s

- Open Directories Found with Golismero BruteForce.

Vulnerability Threat Level: Medium

Vulnerability Definition

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

Vulnerability Remediation

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

[? < 30s] Deploying 75/80.0 | Checks for ASP.net Elmah Logger . . ...Completed in 1s

[? < 40s] Deploying 76/80.0 | Golismero - Checks only for Heartbleed Vulnerability. . . ...Completed in 1s

- HEARTBLEED Vulnerability Found with Golismero.

Vulnerability Threat Level: High

Vulnerability Definition

This vulnerability seriously leaks private information of your host. An attacker can keep the TLS connection alive and can retrieve a maximum of 64K of data per heartbeat.

Vulnerability Remediation

PFS (Perfect Forward Secrecy) can be implemented to make decryption difficult. Complete remediation and resource information is available here. http://heartbleed.com/

[? < 30s] Deploying 77/80.0 | Nmap [Heartbleed] - Checks only for Heartbleed Vulnerability. . . ...Completed in 1s

[? < 20s] Deploying 78/80.0 | Nmap [XSS Filter Check] - Checks if XSS Protection Header is present. . . ...Completed in 1s

[? < 35s] Deploying 79/80.0 | Nikto - Performs SSL Checks. . . ...Completed in 1s

- Vulnerabilities reported in SSL Scans.

Vulnerability Threat Level: Medium

Vulnerability Definition

SSL related vulnerabilities breaks the confidentiality factor. An attacker may perform a MiTM attack,

intrepret and eavesdrop the communication.

Vulnerability Remediation

Proper implementation and upgraded version of SSL and TLS libraries are very critical when it comes to blocking SSL related vulnerabilities.

[? < 35s] Deploying 80/80.0 | Nikto - Checks for Server Issues. . . . ...Completed in 1s

- Some issues found on the Webserver.

Vulnerability Threat Level: Medium

Vulnerability Definition

Particular Scanner found multiple vulnerabilities that an attacker may try to exploit the target.

Vulnerability Remediation

Refer to RS-Vulnerability-Report to view the complete information of the vulnerability, once the scan gets completed.

[Preliminary Scan Phase Completed.]

[Report Generation Phase Initiated.]

Complete Vulnerability Report for iclan.cm named `RS-Vulnerability-Report` is available under the same directory RapidScan resides.

Total Number of Vulnerability Checks : 80

Total Number of Vulnerability Checks Skipped: 0

Total Number of Vulnerabilities Detected : 29

Total Time Elapsed for the Scan : 9s

For Debugging Purposes, You can view the complete output generated by all the tools named `RS-Debug-ScanLog` under the same directory.

[Report Generation Phase Completed.]