Our Findings

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

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.

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.

Found Subdomains with Fierce.
Vulnerability Threat Level: Medium
Vulnerability Definition

Our Findings

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.

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

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.

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.

Our Findings

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.

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/

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

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

Our Findings

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.

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.

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.

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/

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

Our Findings

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.

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/

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.

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.

HTTP PUT DEL Methods Enabled.

Our Findings

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/

 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.

 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 detailed report to view the complete information of the vulnerability, once the scan gets completed.

 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 detailed report to view the complete information of the vulnerability, once the scan gets completed.

 Email Addresses Found.
Vulnerability Threat Level: Low
Vulnerability Definition

Our Findings

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.

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

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.

Webserver vulnerable to Shellshock Bug.

Vulnerability Threat Level: Critical

Vulnerability Definition

Our Findings

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

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.

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.

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

Our Findings

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 : 8s