Practice Website

Vulnerability Scan Report

Test URL: http://testfire.net

65.61.137.117

0	0	2	1	23
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
LOW	3.7	4.5	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
INFO	N/A	-	46180	Additional DNS Hostnames
INFO	N/A	-	39446	Apache Tomcat Detection
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported

Vulnerability Name: Insecure TLS Protocol (TLS 1.0)

CWE: CWE-326 (Inadequate Encryption Strength)

OWASP Category: OWASP Top Ten - A6: Security Misconfiguration

Description: The vulnerability involves the use of TLS version 1.0, an outdated and insecure cryptographic protocol, for securing communications between the client and server. TLS 1.0 has known vulnerabilities, including susceptibility to attacks such as POODLE (Padding Oracle On Downgraded Legacy Encryption), which can compromise the confidentiality and integrity of data transmitted over the network.

Business Impact: Using TLS 1.0 exposes the system to potential eavesdropping, man-in-the-middle attacks, and data tampering. Attackers could exploit vulnerabilities in TLS 1.0 to intercept sensitive data, compromise user sessions, and impersonate legitimate users or servers. The business impact includes potential data breaches, loss of customer trust, regulatory non-compliance (as many regulations require secure communication protocols), and legal consequences if sensitive information is compromised. It's crucial to upgrade to a more secure TLS version (such as TLS 1.2 or higher) to mitigate these risks.

Vulnerability Name: Deprecated TLS Protocol Version (TLS 1.1)

CWE: CWE-326 (Inadequate Encryption Strength)

OWASP Category: OWASP Top Ten - A6: Security Misconfiguration

Description: The vulnerability involves the use of TLS version 1.1, which is deprecated and considered insecure. Deprecated protocols are older versions that have known vulnerabilities and should not be used for securing communications between the client and server. TLS 1.1 has known weaknesses, and continued use of this version can put the system at risk of attacks, compromising the confidentiality and integrity of data transmitted over the network.

Business Impact: Continuing to use deprecated TLS 1.1 exposes the system to potential eavesdropping, man-in-the-middle attacks, and data tampering. Attackers could exploit vulnerabilities in TLS 1.1 to intercept sensitive data, compromise user sessions, and impersonate legitimate users or servers. The business impact includes potential data breaches, loss of customer trust, regulatory non-compliance (as many regulations require secure communication protocols), and legal consequences if sensitive information is compromised. It's crucial to upgrade to a more secure TLS version (such as TLS 1.2 or higher) to mitigate these risks.

Vulnerability Name: Logjam Attack

CWE: CWE-326 (Inadequate Encryption Strength)

OWASP Category: OWASP Top Ten - A6: Security Misconfiguration

Description: The Logjam attack is a vulnerability that arises when a server and client negotiate to use Diffie-Hellman key exchange with a key size of 1024 bits or lower. This small key size makes it feasible for attackers to perform precomputation and then derive the shared keys used for secure communication. Attackers can exploit this vulnerability to intercept and tamper with encrypted communication between the client and server.

Business Impact: Logjam attacks can lead to the compromise of sensitive data, including login credentials, financial information, or other confidential data transmitted over the network. Attackers can potentially decrypt intercepted traffic, leading to unauthorized access, data breaches, loss of customer trust, and reputational damage. To mitigate this vulnerability, it is crucial to use stronger Diffie-Hellman key sizes (2048 bits or higher) and to ensure that all parties involved in the communication support modern cryptographic standards

Vulnerability Name: Missing HTTP Strict Transport Security (HSTS) Header

CWE: CWE-319 (Cleartext Transmission of Sensitive Information)

OWASP Category: OWASP Top Ten - A6: Security Misconfiguration

Description: HTTP Strict Transport Security (HSTS) is a security policy mechanism that helps to protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking. When the HSTS header is missing from an HTTPS server, it means the server is not instructing the client web browser to only use secure, encrypted connections (HTTPS) for all future communication with the site. This leaves the site vulnerable to SSL-stripping attacks, where an attacker can potentially downgrade the connection to HTTP and intercept sensitive data.

Business Impact: Without HSTS, sensitive data transmitted between the client and server can be intercepted, leading to potential unauthorized access, data breaches, session hijacking, and other security threats. Additionally, without HSTS, the website may be susceptible to man-in-the-middle attacks, leading to reputational damage, loss of customer trust, legal consequences, and financial losses if sensitive information is compromised. Implementing HSTS helps ensure a more secure and trusted connection between the client and server.

Vulnerability Name: Weak Hashing Algorithm in SSL Certificate

CWE: CWE-326 (Inadequate Encryption Strength)

OWASP Category: OWASP Top Ten - A6: Security Misconfiguration

Description: This vulnerability occurs when an SSL certificate is signed using a weak hashing algorithm, such as MD5 or SHA-1. Weak hashing algorithms are susceptible to collision attacks, where two different inputs can produce the same hash value. This vulnerability undermines the integrity of the SSL certificate, making it easier for attackers to forge a certificate and perform man-in-the-middle attacks, intercepting and altering encrypted communication between the client and server.

Business Impact: An SSL certificate signed with a weak hashing algorithm can be exploited by attackers to impersonate a legitimate website, leading to unauthorized access, data theft, session hijacking, and other malicious activities. It undermines the trust users place in the security of the website. Additionally, the website could face legal consequences and financial losses if sensitive information is compromised. To mitigate this vulnerability, it is essential to use strong hashing algorithms, such as SHA-256 or higher, for SSL certificate signatures.

Vulnerability Name: Clickjacking

CWE: CWE-451 (User Interface (UI) Misrepresentation of Critical Information)

OWASP Category: OWASP Top Ten - A6: Security Misconfiguration

Description: Clickjacking is a type of attack where a malicious website can trick a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or taking control of their actions without their knowledge or consent. The absence of the anti-clickjacking X-Frame-Options header means that the website does not specify that it should not be embedded within an iframe, leaving it vulnerable to clickjacking attacks.

Business Impact: Clickjacking attacks can lead to various malicious activities, such as unauthorized access to sensitive information, performing actions on behalf of the user without their consent, or stealing user credentials. This can result in reputation damage, loss of customer trust, legal consequences, and financial losses due to data breaches or unauthorized transactions.

Vulnerability Name: Cross-Site Scripting (XSS)

CWE: CWE-79 (Improper Neutralization of Input During Web Page Generation)

OWASP Category: OWASP Top Ten - A7: Cross-Site Scripting (XSS)

Description: Cross-Site Scripting (XSS) is a security vulnerability that allows attackers to inject malicious scripts into web pages viewed by users. When the X-XSS-Protection header is not defined, the user agent (such as a web browser) may not have specific instructions to protect against certain forms of XSS attacks. Without this header, malicious scripts can be injected into the web application, potentially leading to the execution of arbitrary code in the context of the user's browser session.

Business Impact: XSS attacks can lead to unauthorized access, theft of sensitive data, session hijacking, defacement of websites, and potentially spreading malware to site visitors. This can result in reputational damage, loss of customer trust, legal liabilities, and financial losses due to legal consequences or theft of sensitive information.

Vulnerability Name: MIME Sniffing / Content Type Mismatch

CWE: CWE-116 (Improper Encoding or Escaping of Output)

OWASP Category: OWASP Top Ten - A6: Security Misconfiguration

Description: MIME Sniffing, also known as Content Type Mismatch, occurs when the Content-Type header sent by the server doesn't match the actual content of the file. In this case, the absence of the X-Content-Type-Options header allows browsers to interpret files in a different way than intended. Browsers might attempt to determine the content type of a response based on the content itself, leading to potential security risks, especially when dealing with certain file types like scripts or executables.

Business Impact: MIME Sniffing vulnerabilities can lead to various attacks, such as script injection, data theft, or content spoofing. If a browser interprets a file as a different content type (e.g., treating an executable file as a script), it can result in unexpected behaviors, potentially allowing attackers to execute malicious code in the context of the user's session. This can lead to unauthorized access, data breaches, loss of customer trust, and reputational damage.

Vulnerability Name: Directory Listing

CWE: CWE-548 (Exposure of Information Through Directory Listing)

OWASP Category: OWASP Top Ten - A5: Security Misconfiguration

Description: Directory Listing vulnerability occurs when a web server does not have an index file (like index.html or index.php) in a directory, and directory listing is not disabled. As a result, when a user accesses a directory without specifying a particular file, the server may list the

contents of the directory, revealing sensitive information about the server's file structure and potentially exposing files or directories that were not meant to be public.

Business Impact: Directory Listing can provide attackers with valuable information, such as the names of files, directories, or technologies in use. This information can be leveraged in various attacks, including directory traversal attacks, information gathering for social engineering attacks, or targeted attacks against specific files. It can also lead to disclosure of sensitive data, loss of intellectual property, and reputational damage if sensitive information is exposed to unauthorized parties.