Vulnerability Assessment Report

Executive Summary:

This report provides a comprehensive vulnerability assessment of the network infrastructure and web applications associated with the domain veltech.edu.in and its subdomains. The assessment identifies several critical vulnerabilities across various components of the infrastructure, including server software, web technologies, and subdomains. The vulnerabilities range from outdated software versions to configuration weaknesses, potentially exposing the network to various cyber threats such as cross-site scripting (XSS), SSL certificate expiry, email header injection, and more. Recommendations are provided to mitigate these vulnerabilities and enhance the overall security posture of the network.

1. Server Software and Technology:

The following software and technologies have been identified:

Google Analytics GA4
MySQL
PHP
Cloudflare
Elementor 3.18.3
Font Awesome
Bootstrap
Elementor Header & Footer Builder
jQuery Migrate 3.4.1
HTTP/3
jQuery
OWL Carousel
Vue.js
Webpack
Module Federation
WordPress
Slider Revolution
Risk Description:

Risk Description: Exposure of specific software types and versions could aid attackers in crafting targeted attacks against known vulnerabilities associated with these technologies.
Recommendation:

Recommendation: Remove or obfuscate information that discloses software platform, technology, server, and operating system details from HTTP server headers, HTML meta tags, etc.

2. Subdomains: The domain veltech.edu.in encompasses various subdomains, each serving different purposes. Below is a comprehensive overview of the identified subdomains along with their corresponding IP addresses:

www.apps.veltech.edu.in (3.7.225.253)
server2.veltech.edu.in (3.7.225.253)
apps.veltech.edu.in (3.7.225.253)
test.veltech.edu.in (13.201.210.87)
webdisk.veltech.edu.in (13.201.210.87)
www.auto.veltech.edu.in (13.201.210.87)
cpcontacts.veltech.edu.in (13.201.210.87)
auto.veltech.edu.in (13.201.210.87)
ns1.veltech.edu.in (13.201.210.87)
server1.veltech.edu.in (13.201.210.87)
www.test.veltech.edu.in (13.201.210.87)
cpcalendars.veltech.edu.in (13.201.210.87)
cpanel.veltech.edu.in (13.201.210.87)
www.it.veltech.edu.in (13.201.210.87)
webmail.veltech.edu.in (13.201.210.87)
it.veltech.edu.in (13.201.210.87)
ns.veltech.edu.in (27.251.102.100)
application.veltech.edu.in (65.0.22.196)
ftp.veltech.edu.in (104.21.78.95)
ns2.veltech.edu.in (104.21.78.95)
alumni.veltech.edu.in (104.21.78.95)
veltech.edu.in (172.67.219.101)
mail.veltech.edu.in (172.67.219.101)
www.veltech.edu.in (172.67.219.101)
img.veltech.edu.in (202.162.245.200)
email.veltech.edu.in (216.239.32.21)

Risk Description:
Subdomains may introduce potential attack vectors and security risks, including but not limited to misconfigurations, outdated software, and unauthorized access.

Recommendation:

Regularly scan and assess the security posture of all subdomains.
Ensure proper configuration and patch management to mitigate vulnerabilities.
Implement strong access controls and monitoring mechanisms to prevent unauthorized access.
Consider consolidating and optimizing subdomains to reduce attack surface and administrative overhead.

3. Identified Vulnerabilities:

PHP Unsupported Version Detection

Vulnerability ID: 58987
Title: PHP Unsupported Version Detection
Synopsis: The remote host contains an unsupported version of a web application scripting language.
Risk Factor: Critical

Description:
The installation of PHP on the remote host is identified to be version 7.2.30, which is no longer supported by the vendor. Lack of vendor support implies that no new security patches for the product will be released. Consequently, this unsupported version of PHP is likely to contain security vulnerabilities, exposing the system to potential exploitation by malicious actors.

Recommendation:
It is strongly advised to upgrade to a version of PHP that is currently supported by the vendor. The supported versions include 8.0.x and 8.1.x. Upgrading to a supported version will ensure that the system receives security patches and updates, thereby reducing the risk of security breaches and potential compromise.

Solution:
Upgrade PHP to a version that is currently supported, such as PHP 8.0.x or PHP 8.1.x. Ensure that all dependencies and compatibility issues are addressed during the upgrade process.

References:
- [PHP End of Life (EOL) Policy](http://php.net/eol.php)
- [PHP Supported Versions](http://php.net/supported-versions.php)

CVSS Metrics:
- CVSS v3.0 Base Score: 10.0 (Critical)
  - AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- CVSS v2.0 Base Score: 10.0 (Critical)
  - AV:N/AC:L/Au:N/C:C/I:C/A:C

Plugin Information:
- Published: 2012/05/04
- Modified: 2022/12/07

Host Affected:
- IP Address: 3.7.225.253
- Port/Service: tcp/2083/www

SSL Medium Strength Cipher Suites Supported (SWEET32)

- Vulnerability ID: 42873
- Title: SSL Medium Strength Cipher Suites Supported (SWEET32)
- Synopsis: The remote service supports the use of medium strength SSL ciphers.
- **Risk Factor: Medium**

Description:
The remote host supports the use of SSL ciphers that provide medium strength encryption. Medium strength encryption is defined as any encryption that uses key lengths greater than or equal to 64 bits and less than 112 bits, or utilizes the 3DES encryption suite. It is important to note that medium strength encryption can be easier to circumvent, especially if the attacker is on the same physical network.

Recommendation:
It is recommended to reconfigure the affected application to avoid the use of medium strength ciphers. This can be achieved by updating the SSL configuration to disable medium strength ciphers and prefer stronger encryption algorithms. Additionally, consider upgrading to newer versions of SSL/TLS protocols that offer enhanced security features.

Solution:
Reconfigure the affected application, if possible, to eliminate the use of medium strength ciphers. Update the SSL/TLS configuration to prioritize strong encryption algorithms and disable medium strength ciphers such as 3DES.

References:
- [CVE-2016-2183](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2183)
- [OpenSSL Blog - SWEET32 Vulnerability](https://www.openssl.org/blog/blog/2016/08/24/sweet32/)
- [SWEET32 Information](https://sweet32.info)

CVSS Metrics:
- CVSS v3.0 Base Score: 7.5 (Medium)
  - AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
- CVSS v2.0 Base Score: 5.0 (Medium)
  - AV:N/AC:L/Au:N/C:P/I:N/A:N

Plugin Information:
- Published: 2009/11/23
- Modified: 2021/02/03

Affected Hosts:
1. IP Address: 115.240.192.155
   - Port/Service: tcp/1433/mssql
   - Cipher Suite: DES-CBC3-SHA (3DES-CBC(168))

2. IP Address: 115.240.192.155
   - Port/Service: tcp/3389/msrdp
   - Cipher Suite: DES-CBC3-SHA (3DES-CBC(168))

PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability

- Vulnerability ID: 140532
- Title: PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability
- Synopsis: The version of PHP running on the remote web server is affected by a memory leak vulnerability.
- **Risk Factor: Medium**

Description:
The version of PHP installed on the remote web server is reported to be 7.2.x or 7.3.x prior to 7.3.22. This version is affected by a memory leak vulnerability within the LDAP component. An unauthenticated remote attacker could potentially exploit this vulnerability to trigger a denial-of-service condition, leading to service disruption or system unavailability.

Recommendation:
To mitigate this vulnerability, it is strongly advised to upgrade the PHP installation to version 7.3.22 or later. This upgrade includes fixes to address the memory leak vulnerability present in earlier versions. Additionally, consider implementing proactive monitoring and resource management practices to detect and mitigate potential memory-related issues.

Solution:
Upgrade PHP to version 7.3.22 or later to remediate the memory leak vulnerability. Ensure that all necessary dependencies and configurations are updated accordingly to maintain system integrity and security.

References:
- [PHP ChangeLog - Version 7.3.22](https://www.php.net/ChangeLog-7.php#7.3.22)
- [IAVA:2020-A-0420-S](reference not provided)

CVSS Metrics:
- CVSS v3.0 Base Score: 7.5 (Medium)
  - AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v2.0 Base Score: 5.0 (Medium)
  - AV:N/AC:L/Au:N/C:N/I:N/A:P

Plugin Information:
- Published: 2020/09/11
- Modified: 2022/04/11

Affected Host:
- IP Address: 3.7.225.253
  - URL: https://ec2-3-7-225-253.ap-south-1.compute.amazonaws.com:2083/
  - Installed PHP Version: 7.2.30
  - Fixed PHP Version: 7.3.22

PHP < 7.3.24 Multiple Vulnerabilities

- Vulnerability ID: 142591
- Title: PHP < 7.3.24 Multiple Vulnerabilities
- Synopsis: The version of PHP running on the remote web server is affected by multiple vulnerabilities.
- **Risk Factor: Medium**

Description:
The PHP version installed on the remote web server is reported to be prior to 7.3.24. As a result, it is susceptible to multiple vulnerabilities. These vulnerabilities pose a risk to the security and integrity of the web server, potentially enabling attackers to exploit various security weaknesses and compromise the system.

Recommendation:
To mitigate these vulnerabilities, it is highly recommended to upgrade the PHP installation to version 7.3.24 or later. Upgrading to the latest supported version will address the identified vulnerabilities and enhance the overall security posture of the web server. Additionally, ensure that all necessary configurations and dependencies are updated to maintain compatibility and security.

Solution:
Upgrade PHP to version 7.3.24 or later to remediate the identified vulnerabilities and strengthen the security of the web server. Regularly monitor for security advisories and apply patches promptly to address any future vulnerabilities that may arise.

References:
- [PHP ChangeLog - Version 7.3.24](https://www.php.net/ChangeLog-7.php#7.3.24)
- [IAVA:2020-A-0510-S](reference not provided)

CVSS Metrics:
- CVSS v3.0 Base Score: 7.5 (Medium)
  - AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v2.0 Base Score: 5.0 (Medium)
  - AV:N/AC:L/Au:N/C:N/I:N/A:P

Plugin Information:
- Published: 2020/11/06
- Modified: 2022/04/11

Affected Host:
- IP Address: 3.7.225.253
  - URL:
https://ec2-3-7-225-253.ap-south-1.compute.amazonaws.com:2083/
  - Installed PHP Version: 7.2.30
  - Fixed PHP Version: 7.3.24

Apache 2.4.x < 2.4.58 Multiple Vulnerabilities

- Vulnerability ID: 183391
- Title: Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
- Synopsis: The remote web server is affected by multiple vulnerabilities.
- **Risk Factor: High**

Description:
The version of Apache httpd installed on the remote host is reported to be prior to 2.4.58. Consequently, it is susceptible to multiple vulnerabilities, as outlined in the 2.4.58 advisory:
1. mod_macro buffer over-read: Apache HTTP Server's mod_macro is vulnerable to an Out-of-bounds Read issue, impacting versions through 2.4.57. This vulnerability, identified as CVE-2023-31122, could be exploited by an attacker to execute arbitrary code.
2. DoS in HTTP/2 with initial window size 0: Apache HTTP Server is susceptible to a Denial-of-Service (DoS) vulnerability in HTTP/2 connections with an initial window size of 0, affecting versions from 2.4.55 through 2.4.57. An attacker could exploit this to exhaust worker resources, leading to a server outage. This vulnerability is referenced as CVE-2023-43622.
3. HTTP/2 stream memory not reclaimed right away on RST: Another flaw affecting Apache HTTP Server in versions 2.4.55 through 2.4.57 allows a client to cause memory consumption growth by keeping connections busy with new requests and resets. This vulnerability, designated as CVE-2023-45802, could lead to memory exhaustion and service disruption.

Recommendation:
To mitigate these vulnerabilities, it is imperative to upgrade the Apache installation to version 2.4.58 or later. The latest version addresses the identified vulnerabilities and enhances the server's resilience against potential exploits. Regularly monitor for security advisories and apply updates promptly to maintain a secure web server environment.

Solution:
Upgrade Apache to version 2.4.58 or later to remediate the identified vulnerabilities and fortify the security posture of the web server. Promptly address any security patches or updates released by the Apache Software Foundation to safeguard against emerging threats.

References:
- [Apache HTTP Server 2.4.58 Release Notes](reference not provided)
- [CVE-2023-31122](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-31122)
- [CVE-2023-43622](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-43622)
- [CVE-2023-45802](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-45802)
- [IAVB:2023-B-0083](reference not provided)
- [IAVA:2023-A-0572](reference not provided)

CVSS Metrics:
- CVSS v3.0 Base Score: 7.5 (High)
  - AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v3.0 Temporal Score: 6.5
  - CVSS:3.0/E:U/RL:O/RC:C
- CVSS v2.0 Base Score: 7.8 (High)
  - AV:N/AC:L/Au:N/C:N/I:N/A:C

- CVSS v2.0 Temporal Score: 5.8
  - CVSS2#E:U/RL:OF/RC:C

Plugin Information:
- Published: 2023/10/19
- Modified: 2023/11/02

Affected Host:
- IP Address: 3.7.225.253
  - URL: https://ec2-3-7-225-253.ap-south-1.compute.amazonaws.com/
  - Installed Apache Version: 2.4.57
  - Fixed Apache Version: 2.4.58

SSL Certificate Cannot Be Trusted

- Vulnerability ID: 51192 (6)
- Title: SSL Certificate Cannot Be Trusted
- Synopsis: The SSL certificate for this service cannot be trusted.
- **Risk Factor: Medium**

Description:
The SSL certificate for the identified services is deemed untrustworthy due to various reasons:
1. Expired Certificates: The certificates provided by the remote host have expired, leading to a break in the chain of trust. This situation can undermine the authenticity and integrity of the SSL/TLS connections established with clients.
   - Expiry Details:
     - Subject: O=Digital Signature Trust Co./CN=DST Root CA X3
     - Not After: Sep 30 14:01:15 2021 GMT
2. Unknown Certificate Authority: Some certificates are signed by an unknown certificate authority, raising concerns about the legitimacy of the certificates and the security of the communication channel.
   - Example:
     - Issuer: CN=SSL_Self_Signed_Fallback
     - Subject: CN=SSL_Self_Signed_Fallback

Impact:
The presence of untrusted SSL certificates poses several risks:
- Increases the difficulty for users to verify the authenticity and identity of the web server, potentially facilitating man-in-the-middle attacks.
- Undermines the confidentiality and integrity of data transmitted over SSL/TLS connections, exposing sensitive information to eavesdropping and tampering.

Recommendation:

To mitigate this vulnerability, the following actions are recommended:
- Renew Certificates: Ensure that SSL certificates are renewed before their expiration dates to maintain continuous trust and security in SSL/TLS connections.
- Acquire Valid Certificates: Purchase or obtain SSL certificates from recognized certificate authorities to establish trust and secure communications with clients.
- Review Certificate Authorities: Validate the certificate authority (CA) used to sign SSL certificates and ensure it is reputable and trusted by client devices.

Solution:
Address the SSL certificate issues by renewing expired certificates and acquiring valid certificates from reputable certificate authorities. Implement robust certificate management practices to maintain the integrity and trustworthiness of SSL/TLS connections.

References:
- [ITU-T Recommendation X.509](https://www.itu.int/rec/T-REC-X.509/en)
- [X.509 - Wikipedia](https://en.wikipedia.org/wiki/X.509)

CVSS Metrics:
- CVSS v3.0 Base Score: 6.5 (Medium)
  - AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
- CVSS v2.0 Base Score: 6.4 (Medium)
  - AV:N/AC:L/Au:N/C:P/I:P/A:N

Plugin Information:
- Published: 2010/12/15
- Modified: 2020/04/27

Affected Hosts:
1. IP Address: 3.7.225.253
   - Ports: 21, 443, 2083
2. IP Address: 115.240.192.138
   - Port: 443
3. IP Address: 115.240.192.155
   - Ports: 1433 (mssql), 3389 (msrdp)

TLS Version 1.0 Protocol Detection

- Vulnerability ID: 104743 (3)
- Title: TLS Version 1.0 Protocol Detection
- Synopsis: The remote service encrypts traffic using an older version of TLS.
- **Risk Factor: Medium**

Description:
The remote service allows connections encrypted using TLS 1.0, an outdated version of the TLS protocol known to have cryptographic vulnerabilities. While modern implementations of TLS 1.0 may mitigate some of these flaws, newer versions such as TLS 1.2 and 1.3 are designed to address these issues more effectively. As of March 31, 2020, endpoints not supporting TLS 1.2 and higher may encounter

compatibility issues with major web browsers and vendors. PCI DSS v3.2 mandates the disabling of TLS 1.0, except for specific terminals and termination points verified as secure against known exploits.

Impact:
Enabling TLS 1.0 poses several risks:
- Cryptographic Weaknesses: TLS 1.0 suffers from cryptographic design flaws that could be exploited by attackers to compromise the confidentiality and integrity of encrypted communications.
- Compatibility Issues: Endpoints relying solely on TLS 1.0 may experience compatibility issues with modern web browsers and vendors, potentially leading to service disruptions and diminished user experience.
- Non-Compliance: Failure to disable TLS 1.0 may result in non-compliance with industry standards such as PCI DSS v3.2, exposing the organization to regulatory penalties and reputational damage.

Recommendation:
To mitigate this vulnerability, it is recommended to:
- Enable TLS 1.2 and 1.3: Upgrade the server to support TLS 1.2 and 1.3, which offer enhanced security and improved cryptographic algorithms.
- Disable TLS 1.0: Configure the server to disable support for TLS 1.0 to prevent its usage and mitigate associated security risks.
- Verify Compatibility: Ensure that the server's applications and services are compatible with TLS 1.2 and higher to avoid compatibility issues with clients and other systems.
- Compliance Verification: Validate compliance with relevant standards such as PCI DSS v3.2 to ensure adherence to industry best practices and regulatory requirements.

Solution:
Implementing support for TLS 1.2 and 1.3 while disabling TLS 1.0 helps enhance the security posture of the server and ensures compatibility with modern web standards. By following best practices for TLS configuration, organizations can mitigate the risk of cryptographic vulnerabilities and maintain compliance with industry regulations.

References:
- [Draft: Deprecating TLS 1.0 and 1.1](https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00)

CVSS Metrics:
- CVSS v3.0 Base Score: 6.5 (Medium)
  - AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N
- CVSS v2.0 Base Score: 6.1 (Medium)
  - AV:N/AC:H/Au:N/C:C/I:P/A:N

Plugin Information:
- Published: 2017/11/22
- Modified: 2023/04/19

Affected Hosts:
1. IP Address: 3.7.225.253
   - Port: 2083 (www)
2. IP Address: 115.240.192.155
   - Ports: 1433 (mssql), 3389 (msrdp)

TLS Version 1.1 Protocol Deprecated

- Vulnerability ID: 157288 (3)
- Title: TLS Version 1.1 Protocol Deprecated
- Synopsis: The remote service encrypts traffic using an older version of TLS.
- **Risk Factor: Medium**

Description:
The remote service allows connections encrypted using TLS 1.1, an outdated version of the TLS protocol. TLS 1.1 lacks support for current and recommended cipher suites, including those that support encryption before MAC computation and authenticated encryption modes such as GCM. As of March 31, 2020, endpoints not supporting TLS 1.2 and higher may encounter compatibility issues with major web browsers and vendors.

Impact:
Enabling TLS 1.1 poses several risks:
- Limited Cipher Suite Support: TLS 1.1 lacks support for modern cipher suites, limiting the encryption options available and potentially weakening the security of encrypted communications.
- Compatibility Issues: Endpoints relying solely on TLS 1.1 may experience compatibility issues with modern web browsers and vendors, leading to service disruptions and diminished user experience.
- Non-Compliance: Failure to upgrade to TLS 1.2 or 1.3 may result in non-compliance with industry standards, exposing the organization to regulatory penalties and reputational damage.

Recommendation:
To mitigate this vulnerability, it is recommended to:
- Enable TLS 1.2 and/or 1.3: Upgrade the server to support TLS 1.2 and/or 1.3, which offer enhanced security and improved cryptographic algorithms.
- Disable TLS 1.1: Configure the server to disable support for TLS 1.1 to prevent its usage and mitigate associated security risks.
- Verify Compatibility: Ensure that the server's applications and services are compatible with TLS 1.2 and higher to avoid compatibility issues with clients and other systems.
- Compliance Verification: Validate compliance with relevant standards and regulations to ensure adherence to industry best practices.

Solution:
Implementing support for TLS 1.2 and/or 1.3 while disabling TLS 1.1 helps enhance the security posture of the server and ensures compatibility with modern web standards.

References:
- [RFC 8996: Deprecating TLSv1.0 and TLSv1.1](https://datatracker.ietf.org/doc/html/rfc8996)

CVSS Metrics:
- CVSS v3.0 Base Score: 6.5 (Medium)
  - AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N
- CVSS v2.0 Base Score: 6.1 (Medium)
  - AV:N/AC:H/Au:N/C:C/I:P/A:N

Plugin Information:
- Published: 2022/04/04
- Modified: 2023/04/19

Affected Hosts:
1. IP Address: 3.7.225.253
   - Port: 2083 (www)
2. IP Address: 115.240.192.155
   - Ports: 1433 (mssql), 3389 (msrdp)

SSL Self-Signed Certificate

- Vulnerability ID: 57582 (2)
- Title: SSL Self-Signed Certificate
- Synopsis: The SSL certificate chain for this service ends in an unrecognized self-signed certificate.
- **Risk Factor: Medium**

Description:
The SSL certificate chain for the identified service ends with a self-signed certificate that is not recognized by any trusted certificate authority. A self-signed certificate lacks the validation provided by a recognized certificate authority, making it susceptible to man-in-the-middle attacks. This vulnerability nullifies the use of SSL for securing communications, especially if the affected host is a public-facing server in a production environment.

Impact:
The presence of self-signed certificates poses several risks:
- Man-in-the-Middle Attacks: Attackers can intercept communications between clients and the server, compromising the confidentiality and integrity of transmitted data.
- Security Implications: The use of self-signed certificates undermines the trustworthiness of SSL/TLS encryption, potentially exposing sensitive information to unauthorized access.
- Non-Compliance: Failure to use trusted SSL certificates may lead to non-compliance with security standards and regulations, resulting in regulatory penalties and reputational damage.

Recommendation:
To mitigate this vulnerability, it is recommended to:
- Acquire Trusted SSL Certificates: Purchase or obtain SSL certificates from recognized certificate authorities to ensure the authenticity and integrity of encrypted connections.
- Install Valid Certificates: Replace self-signed certificates with trusted SSL certificates issued by reputable certificate authorities.
- Regular Certificate Renewal: Ensure SSL certificates are regularly renewed before expiration to maintain secure communication channels.
- Configuration Review: Periodically review SSL certificate configurations to detect and remediate any instances of self-signed certificates.

Solution:
Procuring and deploying SSL certificates signed by trusted certificate authorities is essential for establishing secure and trustworthy SSL/TLS connections.

CVSS Metrics:
- CVSS v3.0 Base Score: 6.5 (Medium)
  - AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
- CVSS v2.0 Base Score: 6.4 (Medium)
  - AV:N/AC:L/Au:N/C:P/I:P/A:N

Plugin Information:
- Published: 2012/01/17
- Modified: 2022/06/14

Affected Hosts:
1. IP Address: 115.240.192.155
   - Port: 1433 (mssql)
   - Certificate Subject: CN=SSL_Self_Signed_Fallback
2. IP Address: 115.240.192.155
   - Port: 3389 (msrdp)
   - Certificate Subject: CN=WIN-UVK0L3E8KUG

JQuery 1.2 < 3.5.0 Multiple XSS

- Vulnerability ID: 136929 (2)
- Title: JQuery 1.2 < 3.5.0 Multiple XSS
- Synopsis: The remote web server is affected by multiple cross-site scripting vulnerabilities.
- **Risk Factor: Medium**

Description:
The remote web server hosts a version of JQuery that is equal to or greater than 1.2 and less than 3.5.0, making it vulnerable to multiple cross-site scripting (XSS) attacks. These vulnerabilities can allow attackers to inject malicious scripts into web pages viewed by users, potentially leading to unauthorized data disclosure, session hijacking, and other security compromises. It is essential to address these vulnerabilities promptly to prevent exploitation and protect user data and system integrity.

Impact:
- Cross-Site Scripting (XSS): Attackers can exploit XSS vulnerabilities to execute arbitrary scripts within the context of a user's browser, leading to various security threats such as data theft, session manipulation, and website defacement.
- Data Integrity Compromise: XSS attacks can manipulate or steal sensitive data stored within web applications, compromising the confidentiality and integrity of user information.
- Client-Side Security Risks: Vulnerable JQuery versions expose users to client-side security risks, undermining the trustworthiness of web applications and potentially exposing them to further exploitation.

Recommendation:
To mitigate this vulnerability, it is recommended to:
- Upgrade JQuery: Upgrade the JQuery library to version 3.5.0 or later to address the identified XSS vulnerabilities and benefit from the latest security enhancements.

- Apply Security Patches: Apply security patches provided by the JQuery project or relevant software vendors to mitigate known vulnerabilities and strengthen web application security.
- Implement Input Sanitization: Implement proper input validation and output encoding to prevent XSS attacks and sanitize user-supplied data before rendering it in web pages.
- Security Testing: Conduct regular security testing, including vulnerability scans and code reviews, to identify and remediate XSS vulnerabilities and other security issues proactively.

Solution:
Upgrade the installed version of JQuery to 3.5.0 or later to eliminate the identified XSS vulnerabilities and enhance the security posture of the web server.

CVSS Metrics:
- CVSS v3.0 Base Score: 6.1 (Medium)
  - AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
- CVSS v2.0 Base Score: 4.3 (Medium)
  - AV:N/AC:M/Au:N/C:N/I:P/A:N

Plugin Information:
- Published: 2020/05/28
- Modified: 2023/10/13

Affected Hosts:
1. IP Address: 3.7.225.253
   - Port: 2083 (www)
   - URL: https://ec2-3-7-225-253.ap-south-1.compute.amazonaws.com:2083/login/cwp_theme/original/js/jquery-3.1.1.min.js
   - Installed Version: 3.1.1
   - Fixed Version: 3.5.0
2. IP Address: 104.211.78.76
   - Port: 443 (www)
   - URL: https://104.211.78.76/assest/js/jquery.min.js
   - Installed Version: 1.10.2
   - Fixed Version: 3.5.0

HSTS Missing From HTTPS Server (RFC 6797)

- Vulnerability ID: 142960 (2)
- Title: HSTS Missing From HTTPS Server (RFC 6797)
- Synopsis: The remote web server is not enforcing HSTS (HTTP Strict Transport Security), as defined by RFC 6797.
- **Risk Factor: Medium**

Description:
The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an essential security mechanism that instructs web browsers to communicate only via HTTPS, thereby mitigating downgrade

attacks, SSL-stripping man-in-the-middle attacks, and enhancing protections against cookie hijacking. Without HSTS, the server is vulnerable to various security threats that exploit insecure communication channels and weaken overall security posture.

Impact:
- Downgrade Attacks: Without HSTS, attackers can downgrade HTTPS connections to HTTP, exposing users to interception and manipulation of sensitive data.
- SSL-Stripping MITM Attacks: HSTS helps prevent SSL-stripping man-in-the-middle (MITM) attacks by mandating secure HTTPS connections, reducing the risk of unauthorized data interception.
- Cookie Hijacking Risks: Absence of HSTS weakens protections against cookie hijacking, enabling attackers to steal session cookies and impersonate legitimate users, leading to unauthorized access and potential data breaches.

Recommendation:
To mitigate this vulnerability, it is recommended to:
- Enable HSTS: Configure the remote web server to send the HTTP Strict Transport Security (HSTS) header with an appropriate max-age directive to enforce HTTPS communication.
- Set Max-Age Directive: Specify a sufficiently long max-age directive in the HSTS header to instruct web browsers to cache the HSTS policy for an extended period, ensuring long-term protection against downgrade attacks.
- Include Subdomains: Consider including the includeSubDomains directive in the HSTS header to extend HSTS protection to all subdomains of the web server.
- Preload HSTS: Optionally, submit the web server to the HSTS preload list maintained by major browsers to ensure HSTS enforcement even for first-time visitors.

Solution:
Configure the remote web server to send the HTTP Strict-Transport-Security (HSTS) header with an appropriate max-age directive to enforce HTTPS communication and strengthen security protections against downgrade attacks and SSL-stripping MITM attacks.

CVSS Metrics:
- CVSS v3.0 Base Score: 6.5 (Medium)
  - AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
- CVSS v2.0 Base Score: 5.8 (Medium)
  - AV:N/AC:M/Au:N/C:P/I:P/A:N

Plugin Information:
- Published: 2020/11/17
- Modified: 2024/01/15

Affected Hosts:
- IP Address: 3.7.225.253
  - Port: 443 (www)
  - The remote HTTPS server does not send the HTTP Strict-Transport-Security header.
- IP Address: 3.7.225.253
  - Port: 2083 (www)
  - The remote HTTPS server does not send the HTTP Strict-Transport-Security header.

DNS Server Zone Transfer Information Disclosure (AXFR)

- Vulnerability ID: 10595 (1)
- Title: DNS Server Zone Transfer Information Disclosure (AXFR)
- Synopsis: The remote name server allows DNS zone transfers, potentially disclosing sensitive network information.
- **Risk Factor: Medium**

Description:
The remote name server allows DNS zone transfers to be performed. Zone transfers enable a remote attacker to instantly obtain a list of potential targets within the domain. This information can be leveraged by attackers to map out the network topology, identify potential attack surfaces, and uncover new targets for exploitation. Additionally, domain naming conventions used within the zone transfer may reveal details about the server's primary applications or services, further aiding attackers in their reconnaissance efforts.

Impact:
- Information Disclosure: Zone transfers expose sensitive information about the domain's infrastructure, aiding attackers in identifying potential targets and vulnerabilities within the network.
- Reconnaissance: Attackers can leverage the obtained information to map out the network topology, identify critical assets, and plan targeted attacks more effectively.

Recommendation:
To mitigate this vulnerability, it is recommended to:
- Restrict Zone Transfers: Limit DNS zone transfers to only the servers that require the information, such as secondary DNS servers or authorized hosts.
- Implement Access Controls: Configure access controls and authentication mechanisms to restrict unauthorized access to DNS zone transfer functionality.
- Monitor DNS Traffic: Regularly monitor DNS traffic for unauthorized zone transfer requests and other suspicious activities that may indicate reconnaissance attempts or potential security threats.

Solution:
Implement access controls and restrict zone transfers to authorized servers or hosts to prevent unauthorized disclosure of sensitive network information.

CVSS Metrics:
- CVSS v2.0 Base Score: 5.0 (Medium)
  - AV:N/AC:L/Au:N/C:P/I:N/A:N
- CVSS v2.0 Temporal Score: 4.2 (Medium)
  - E:U/RL:ND/RC:C

Plugin Information:
- Published: 2001/01/16
- Modified: 2018/09/17

Affected Host:
- IP Address: 3.7.225.253

- Port: 53 (dns)
- Domain: server2.veltech.edu.in
- The remote name server allows DNS zone transfers, potentially disclosing sensitive network information.

HTTP TRACE / TRACK Methods Allowed

- Vulnerability ID: 11213 (1)
- Title: HTTP TRACE / TRACK Methods Allowed
- Synopsis: Debugging functions are enabled on the remote web server.
- **Risk Factor: Medium**

Description:
The remote web server supports the TRACE and/or TRACK methods, which are used for debugging web server connections. Allowing these methods poses a security risk as they can be leveraged by attackers to conduct cross-site tracing (XST) attacks, which can lead to information disclosure and other security vulnerabilities.

Impact:
- Information Disclosure: Enabling TRACE and/or TRACK methods can allow attackers to extract sensitive information, such as cookies or authentication tokens, from HTTP headers, leading to potential security breaches.
- Security Risks: Debugging functions enabled by TRACE and TRACK methods may expose the web server to various vulnerabilities, including cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks.

Recommendation:
To mitigate this vulnerability, it is recommended to:
- Disable TRACE and TRACK Methods: Configure the web server to disable the TRACE and TRACK methods to prevent potential security risks associated with debugging functionality.
- Implement Security Controls: Implement additional security controls, such as input validation and output encoding, to mitigate the risk of other web-based vulnerabilities.

Solution:
To disable TRACE and TRACK methods, add the following lines for each virtual host in your configuration file:

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, for Apache versions 1.3.34, 2.0.55, and 2.2, you can disable the TRACE method natively via the 'TraceEnable' directive.

CVSS Metrics:
- CVSS v2.0 Base Score: 5.0 (Medium)
  - AV:N/AC:L/Au:N/C:P/I:N/A:N
- CVSS v2.0 Temporal Score: 3.7 (Medium)
  - E:U/RL:OF/RC:C

Plugin Information:
- Published: 2003/01/23
- Modified: 2023/10/27

Affected Host:
- IP Address: 3.7.225.253
  - Port: 443 (www)
  - Server: Apache/2.4.57 (Unix) OpenSSL/1.0.2k-fips
  - The remote web server allows the TRACE method, potentially exposing it to security risks.

SSL Certificate Expiry

- Vulnerability ID: 15901 (1)
- Title: SSL Certificate Expiry
- Synopsis: The remote server's SSL certificate has already expired.
- **Risk Factor: Medium**

Description:
This vulnerability report indicates that the SSL certificate associated with the remote server has expired. SSL certificates are essential for secure communication over the internet, and an expired certificate can lead to security risks and potential disruptions in service.

Impact:
- Security Risk: An expired SSL certificate can compromise the confidentiality and integrity of data transmitted between clients and the server, exposing sensitive information to potential interception or manipulation by attackers.
- Trustworthiness: Users may perceive the website as untrustworthy or insecure when encountering an expired SSL certificate, leading to loss of credibility and potential loss of business.

Recommendation:
To remediate this vulnerability, it is recommended to:
- Renew SSL Certificate: Purchase or generate a new SSL certificate to replace the expired one. Ensure that the new certificate is properly configured and installed on the server.
- Automate Certificate Management: Implement automated certificate management solutions to monitor certificate expiration dates and renew certificates in a timely manner to prevent service disruptions and security risks.

Solution:
Purchase or generate a new SSL certificate to replace the existing one. Ensure that the new certificate is valid and properly configured with appropriate expiration dates.

CVSS Metrics:
- CVSS v3.0 Base Score: 5.3 (Medium)
  - AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
- CVSS v2.0 Base Score: 5.0 (Medium)
  - AV:N/AC:L/Au:N/C:N/I:P/A:N

Plugin Information:
- Published: 2004/12/03
- Modified: 2021/02/03

Affected Host:
- IP Address: 115.240.192.138
  - Port: 443 (www)
  - The SSL certificate associated with the domain 'apps.veltech.edu.in' has expired.

SSL Anonymous Cipher Suites Supported

- Vulnerability ID: 31705 (1)
- Title: SSL Anonymous Cipher Suites Supported
- Synopsis: The remote service supports the use of anonymous SSL ciphers.
- **Risk Factor: Low**

Description:
This vulnerability report indicates that the remote service supports the use of anonymous SSL ciphers. Anonymous SSL ciphers allow encryption of traffic without requiring SSL certificates, which can be beneficial for quick setup but pose security risks by not verifying the remote host's identity. This vulnerability could expose the service to man-in-the-middle attacks, especially if the attacker is on the same physical network.

Impact:
- Security Risk: Use of anonymous SSL ciphers renders the service vulnerable to man-in-the-middle attacks as it does not provide a means to verify the remote host's identity, potentially compromising the confidentiality of transmitted data.
- Ease of Exploitation: While the risk is considered low, exploitation of this vulnerability becomes considerably easier if the attacker is on the same physical network, as they can intercept and manipulate traffic more easily.

Recommendation:
To remediate this vulnerability, it is recommended to:
- Reconfigure the Affected Application: If possible, reconfigure the affected application to avoid the use of anonymous SSL ciphers. Instead, use SSL ciphers that provide proper authentication and encryption, ensuring the security of communications.

Solution:

Reconfigure the affected application to avoid the use of anonymous SSL ciphers. Utilize SSL ciphers that provide proper authentication and encryption to enhance the security of communications.

CVSS Metrics:
- CVSS v3.0 Base Score: 5.9 (Low)
  - AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
- CVSS v2.0 Base Score: 2.6 (Low)
  - AV:N/AC:H/Au:N/C:P/I:N/A:N

Plugin Information:
- Published: 2008/03/28
- Modified: 2023/10/27

Affected Host:
- IP Address: 3.7.225.253
  - Port: 21 (tcp)
  - The following SSL anonymous ciphers are supported by the remote TCP server:
    - DH-AES128-SHA256
    - DH-AES256-SHA384
    - DH-AES128-SHA256
    - DH-AES256-SHA256

PHP Denial of Service (DoS)

- Vulnerability ID: 136741 (1)
- Title: PHP 7.2.x < 7.2.31 / 7.3.x < 7.3.18, 7.4.x < 7.4.6 Denial of Service (DoS)
- Synopsis: The version of PHP running on the remote web server is affected by a denial of service vulnerability.
- **Risk Factor: Medium**

Description:
The remote web server is running a version of PHP (7.2.x prior to 7.2.31, 7.3.x prior to 7.3.18, or 7.4.x prior to 7.4.6) that is affected by a denial of service (DoS) vulnerability. This vulnerability exists in PHP's HTTP file upload component, where temporary files created during the file upload process are not properly cleaned up. An unauthenticated attacker can exploit this issue by repeatedly submitting uploads with long file or field names, which can exhaust disk space and cause a DoS condition.

Impact:
- Security Risk: The vulnerability could lead to a denial of service condition, causing the affected server to become unresponsive and potentially disrupt its services.
- Ease of Exploitation: This vulnerability is relatively easy to exploit as it only requires an attacker to submit uploads with long file or field names repeatedly.

Recommendation:
To mitigate this vulnerability, it is recommended to:

- Upgrade PHP: Upgrade the PHP installation to version 7.2.31, 7.3.18, 7.4.6, or later to address the vulnerability and ensure proper cleanup of temporary files during the file upload process.

Solution:
Upgrade PHP to version 7.2.31, 7.3.18, 7.4.6, or later to mitigate the vulnerability and prevent potential denial of service attacks.

CVSS Metrics:
- CVSS v3.0 Base Score: 5.3 (Medium)
  - AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
- CVSS v2.0 Base Score: 5.0 (Medium)
  - AV:N/AC:L/Au:N/C:N/I:N/A:P

Plugin Information:
- Published: 2020/05/21
- Modified: 2022/04/11

Affected Host:
- IP Address: 3.7.225.253
  - Port: 2083 (tcp)
  - Installed version: 7.2.30
  - Fixed version: 7.2.31

PHP Multiple Vulnerabilities

- Vulnerability ID: 141355 (1)
- Title: PHP 7.2 < 7.2.34 / 7.3.x < 7.3.23 / 7.4.x < 7.4.11 Multiple Vulnerabilities
- Synopsis: The version of PHP running on the remote web server is affected by multiple vulnerabilities.
- **Risk Factor: Medium**

Description:
The remote web server is running a version of PHP (7.2.x prior to 7.2.34, 7.3.x prior to 7.3.23, or 7.4.x prior to 7.4.11) that is affected by multiple vulnerabilities:
1. Weak Cryptography Vulnerability (CVE-2020-7069): A weakness exists in PHP's openssl_encrypt function due to its failure to utilize all provided IV bytes. This could allow an unauthenticated attacker to compromise the security of the encryption scheme or affect the integrity of encrypted data.
2. Cookie Forgery Vulnerability (CVE-2020-7070): PHP's HTTP processing functionality is susceptible to a cookie forgery vulnerability. An attacker could exploit this to forge HTTP cookies that were supposed to be secure.

Impact:
- Security Risk: These vulnerabilities pose a medium security risk, potentially allowing attackers to compromise the confidentiality and integrity of data processed by the PHP application.
- Ease of Exploitation: Exploiting these vulnerabilities may require some level of technical expertise but could lead to significant security breaches if successfully exploited.

Recommendation:

To mitigate these vulnerabilities, it is recommended to:
- Upgrade PHP: Upgrade the PHP installation to version 7.2.34, 7.3.23, 7.4.11, or later to address the identified vulnerabilities and enhance the security of the PHP environment.

Solution:
Upgrade PHP to version 7.2.34, 7.3.23, 7.4.11, or later to address the vulnerabilities and prevent potential exploitation by attackers.

CVSS Metrics:
- CVSS v3.0 Base Score: 6.5 (Medium)
  - AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
- CVSS v2.0 Base Score: 6.4 (Medium)
  - AV:N/AC:L/Au:N/C:P/I:P/A:N

Plugin Information:
- Published: 2020/10/09
- Modified: 2022/04/11

Affected Host:
- IP Address: 3.7.225.253
  - Port: 2083 (tcp)
  - Installed version: 7.2.30
  - Fixed version: 7.2.34

PHP Email Header Injection

- Vulnerability ID: 152853 (1)
- Title: PHP < 7.3.28 Email Header Injection
- Synopsis: The version of PHP running on the remote web server is affected by an email header injection vulnerability.
- **Risk Factor: Medium**

Description:
The remote web server is running a version of PHP (prior to 7.3.28) that is affected by an email header injection vulnerability. This vulnerability arises from a failure to properly handle CRLF sequences in email header fields. An attacker can exploit this by inserting line feed characters into email headers, allowing them to gain full control over the content of email headers.

Impact:
- Security Risk: The email header injection vulnerability poses a medium security risk, potentially allowing attackers to manipulate email headers and potentially conduct email-based attacks such as phishing or spamming.
- Ease of Exploitation: Exploiting this vulnerability requires minimal technical knowledge, as it involves inserting line feed characters into email headers.

Recommendation:
To mitigate this vulnerability, it is recommended to:

- Upgrade PHP: Upgrade the PHP installation to version 7.3.28 or later to address the vulnerability and enhance the security of the PHP environment.

Solution:
Upgrade PHP to version 7.3.28 or later to address the vulnerability and prevent potential exploitation by attackers.

CVSS Metrics:
- CVSS v3.0 Base Score: 5.3 (Medium)
  - AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
- CVSS v2.0 Base Score: 5.0 (Medium)
  - AV:N/AC:L/Au:N/C:N/I:P/A:N

Plugin Information:
- Published: 2021/08/26
- Modified: 2022/04/11

Affected Host:
- IP Address: 3.7.225.253
  - Port: 2083 (tcp)
  - Installed version: 7.2.30
  - Fixed version: 7.3.28

PHP Use-After-Free Vulnerability

- Vulnerability ID: 139571 (1)
- Title: PHP 7.2.x < 7.2.33 Use-After-Free Vulnerability
- Synopsis: The version of PHP running on the remote web server is affected by a use-after-free vulnerability.
- **Risk Factor: Low**

Description:
The remote web server is running a version of PHP (prior to 7.2.33) that is affected by a use-after-free vulnerability in the `phar_parse` function. This vulnerability stems from mishandling of the `actual_alias` variable, which could lead to arbitrary code execution. An attacker can exploit this issue by dereferencing a freed pointer, potentially resulting in arbitrary code execution.

Impact:
- Security Risk: The use-after-free vulnerability poses a low security risk, as it requires specific conditions to be met for successful exploitation.
- Ease of Exploitation: Exploiting this vulnerability requires detailed knowledge of PHP internals and specific conditions to trigger the use-after-free condition, making it less likely to be exploited in practice.

Recommendation:
To mitigate this vulnerability, it is recommended to:

- Upgrade PHP: Upgrade the PHP installation to version 7.2.33 to address the vulnerability and enhance the security of the PHP environment.

Solution:
Upgrade PHP to version 7.2.33 to address the use-after-free vulnerability and prevent potential exploitation by attackers.

CVSS Metrics:
- CVSS v3.0 Base Score: 3.6 (Low)
  - AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:L
- CVSS v2.0 Base Score: 3.3 (Low)
  - AV:L/AC:M/Au:N/C:P/I:N/A:P

Plugin Information:
- Published: 2020/08/13
- Modified: 2022/04/11

Affected Host:
- IP Address: 3.7.225.253
  - Port: 2083 (tcp)
  - Installed version: 7.2.30
  - Fixed version: 7.2.33