SECUREU
WE MAKE SECURITY ACCESSIBLE

WEB-APP PENETRATION TESTING

SECURITY REPORT

DEMO CORP

DATE : DD MONTH YYYY

VERSION : 1.0

Confidential Document

Email : contact-us@secureu.in **Phone : +91 8010450348** **www.secureu.in**

CONTENTS ...

1. Confidentiality Statement

This document is the exclusive property of Demo Corp and SECUREU. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires the consent of both Demo Corp and SECUREU.

Demo Corp may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

2. Disclaimer

This web application penetration test was performed by passively scanning the domain owned by Demo Corp. Passive scanning as in no invasive techniques was utilized that could cause any disruption of services made available by Demo Corp.

The vulnerabilities identified were not further exploited as this was a passive pentest scan of the domain to identify the vulnerabilities that can be easily detected.

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

3. Contact Information

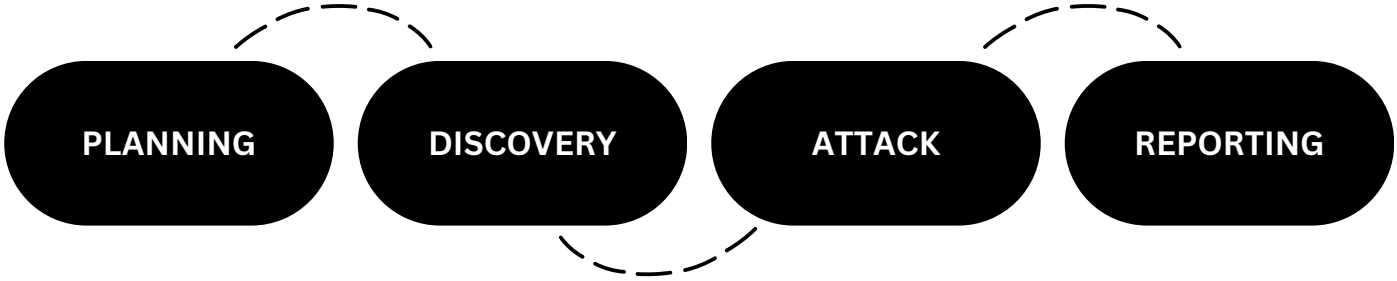
Name	Title	Contact Information
John	Lead Penetration Tester	john@secureu.in
Albert	Security Engineer	albert@secureu.in
Gilbert	Penetration Tester	gilbert@secureu.in

4. Assessment Overview

From <month> xth, 20XX to <month> yth, 20XX SECUREU attempted to evaluate the security posture of the infrastructure of Demo Corp and compared it to the current industry best practices by performing an web application penetration test

Phases of penetration testing activities including the following:

- **Planning** – Customer goals are gathered and rules of engagement obtained.
- **Discovery** – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- **Attack** – Confirm potential vulnerabilities through exploitation and perform additional discoveries upon new access.
- **Reporting** – Document all found vulnerabilities, exploits, failed attempts, and company strengths and weaknesses.



5. Assessment Components

5.1. Webapplication Penetration Test

A web application penetration test emulates the role of an attacker from outside the network. An engineer will scan the assets that face the internet to identify potential vulnerabilities.

6. Finding Severity Ratings

The following table defines levels of severity and the corresponding CVSS score range used throughout the document to assess vulnerability and risk impact.

SEVERITY	CVSS V3 SCORE RANGE	DEFINITIONS
Critical	9.0-10.0	**Exploitation:** • Exploitation is straightforward. • Results in system-level compromise. **Plan of Action:** • Patch immediately.
High	7.0-8.9	**Exploitation**: • Exploitation is more difficult. Could cause elevated privileges. • Potential to cause loss of data or downtime. **Plan of Action**: • Patch as soon as possible.
Medium	4.0-6.9	**Exploitation:** • Vulnerabilities exist but are not exploitable. • Might require extra steps to make the vulnerability exploitable. **Plan of Action**: • Patch after high-priority issues has been resolved.
Low	0.1-3.9	**Exploitation:** • Vulnerabilities are non-exploitable. • Mitigation would reduce an organization's attack surface. **Plan of Action:** • Patch during the next maintenance window.
Informational	N/A	• No vulnerability exists. • Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

7. Risk Factors

Risk is measured by two factors: Likelihood & Impact

7.1. Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, the attacker's skill level, and the client environment.

7.2. Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity and availability of client systems and/or data, reputational harm, and financial loss.

8. Scope

ASSESSMENT	DETAILS
Webapplication Vulnerability Scan	*.democorp.com

8.1. Scope Exclusions

SECUREU did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were covered in penetration testing of the domain

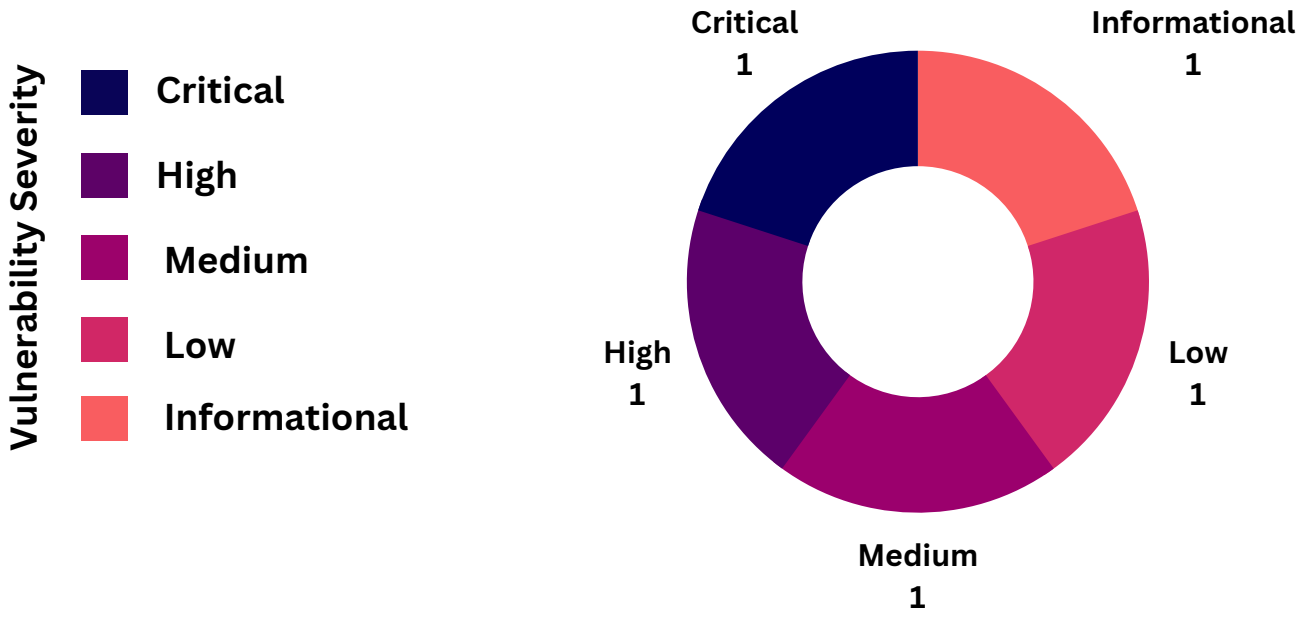
9. Executive Summary

SECUREU evaluated Demo Corp's web application security posture through an external penetration test from <month> xth, 20XX to <month> Yth, 20XX. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

A

Security Rating

VULNERABILITY DISTRIBUTION



9.1. Scoping and Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

9.2. Testing Summary

The web application assessment evaluated **democorp.com's** security posture. The SECUREU team performed vulnerability scanning against the domains mentioned in the scope.

Unrestricted File Upload was found on the domain **democorp.com,** resulting in an attacker being able to **execute commands on the server**. This vulnerability can let an attacker **discover sensitive files** like **databases, password files, and configuration files** which can help an attacker potentially **gain access to the server.**

Also, it was found that the domain **democorp.com does not implement strict HSTS** which means all of the **communications between the user and the webserver are unencrypted.** This can aid an attacker to **gain login credentials, credit/debit card numbers, etc.** By performing **MITM (man in the middle) attacks.**

An **outdated** "**js_composer**" was found on **democorp.com,** the version "**js_composer 5.0.1**" which is implemented is known to be **vulnerable to authenticated stored XSS**, this vulnerability can be utilized by an attacker to **execute arbitrary JavaScript** on the victim's browser.

There were also some vulnerable **old Jquery** libraries being implemented on the website. Usage of these libraries can result in new vulnerabilities arising late

10. Key Strengths and Weaknesses

The following identifies the **key strength**s found during the assessment:

- Use of technologies that have no exploits available out in the open.

The following identifies the **key weaknesses** found during the assessment:

- Good security practices are not being followed.
- Use of outdated technologies.

11. Vulnerability Distribution Table

The following table illustrates the vulnerabilities found by severity and recommended remediations:

FINDINGS	SEVERITY	RECOMMENDATIONS
WPT-001: Contact-form-7 Unrestricted File Upload	**Critical**	Update the Contact-form-7 plugin to the latest version
WPT-002: Authenticated Stored XSS	**Moderate**	Update js_composer to the latest version.
WPT-003: Strict transport policy not enforced	**Low**	Enable HTTP Strict Transport Security (HSTS) by adding a response header
WPT-004: Outdated JQuery libraries	**Informational**	Implement the latest Jquery libraries

12. Web Application Penetration Testing FIndings

WPT-001 : Contact-form-7 Unrestricted File Upload (Critical)

DESCRIPTION:	An outdated version of “Contact-form-7” which is “Contact-form-7 3.51.0” was found, this version was found to be outdated and vulnerable to Unrestricted File Upload. If the server is using file upload functionality anywhere on the site then the attacker can upload a PHP shell on your server.
URL:	http://democorp.com/
APPROACH:	Automated
TOOLS USED:	WPScan
REFERENCES:	Contact Form 7 < 5.3.2 - Unrestricted File Uploadunrestricted-file-upload-in-contact-form-7

Evidence

By visiting the URL we can get the version number of “Contact-form-7” inside source code.

Fig 1: Outdated Contact-form-7

Risk

- **Likelihood**
  If the website is providing the functionality of file upload then it’s highly likely that this vulnerability can be exploited.

- **Impact**

  An attacker can gain remote code execution on the target server by uploading a malicious backdoor. This can be devastating for the company. Depending upon what kind of information or function the affected server serves an attacker can escalate the extent of the damage. Not only this can result in serious security compromise but also damage to the reputation of the organization.

Remediation

Update the Contact-form-7 plugin to the latest version

- **More Information**
  - Latest Releases of Contact-form-7
  - How to fix Contact-form-7 vulnerability

WPT-002: Authenticated Stored XSS (Medium)

DESCRIPTION:	An **outdated** version of "**js-comp-ver 5.0.1**" was found , this version was outdated and vulnerable to **Authenticated Stored XSS.**
URL:	http://democorp.com/
APPROACH:	Automated
TOOLS USED:	WPScan
REFERENCES:	1. Wordfence 2. WPBakery Page Builder XSS

Evidence

By Visiting the URL we can get the version number of **"js-comp-ver**" inside the source code.

Fig 2: Outdated js-comp-ver

Risk

- **Likelihood**
  If the site is using outdated js_composer 5.0.1 then it is highly likely that this site is vulnerable to **Authenticated Stored XSS.**

- **Impact**

  An attacker can execute **arbitrary JavaScript** as the victim user's account. By using this vulnerability attackers can steal **other users' cookies**. Further, this can be chained to **session hijacking.**

Remediation

Update js_composer to the latest version.

- **More Information**
  - How-to-update-js_composer
  - Update WPBakery Page Builder

WPT-003: Strict transport policy not enforced (Low)

DESCRIPTION:	The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to **modify a legitimate user's network traffic** could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users.
URL:	http://democorp.com/
APPROACH:	Manual
TOOLS USED:	N/A
REFERENCES:	1. HSTSpreload 2. Wikipedia HSTS

Evidence

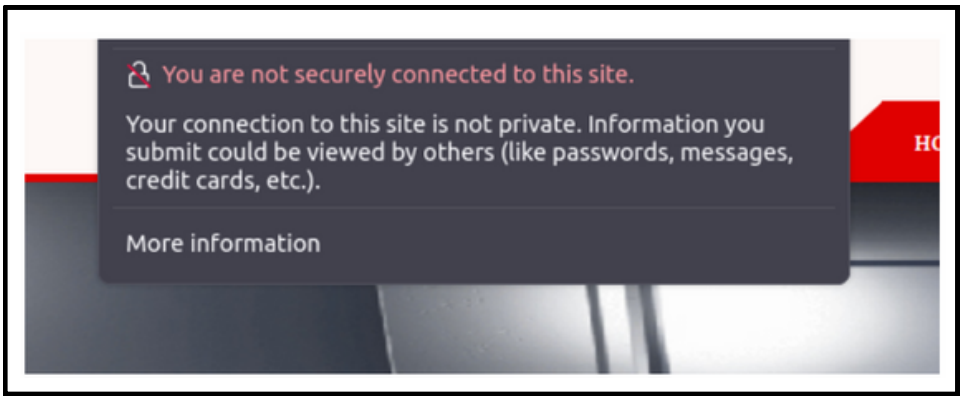


Fig 3: No HSTS

Risk

- **Likelihood**
  As this attack requires the attacker to be in the victim's network it is **not likely** for this attack to happen.

- **Impact**

  If the **attacker is inside** the **victim's network**, he can **potentially downgrade** the **HTTPS protocol to HTTP**, which **results** in an **exchange of data in cleartext**. An attacker can then leverage this vulnerability to **get the cleartext credentials of the victim** if he tries to log in.

Remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where "expireTime" is the time in seconds that the browsers should remember that this particular site should only be accessed using HTTPS. Consider adding the 'include subdomains' flag if appropriate.

- **More Information**
  - What Is HSTS and How Do I Implement It? (globalsign.com)
  - HSTS HeaderExplanation, Examples, and Prevention (crashtest-security.com)

WPT-004: Outdated JQuery libraries (Informational)

DESCRIPTION:	The domain uses an **older version** of the **Jquery Javascript library** named "**jquery 1.12.4**" which has been found to be vulnerable to **Cross-site scripting attacks.**
URL:	http://democorp.com/
APPROACH:	Manual
TOOLS USED:	N/A
REFERENCES:	1.jquery@1.12.4 vulnerabilities

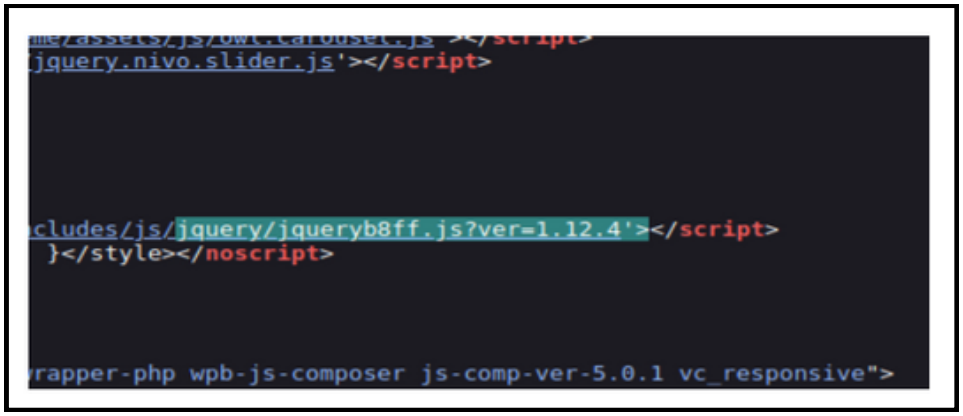


Fig 4: Outdated JS library

Risk

- **Likelihood**

  Not applicable as no vulnerabilities were found.

- **Impact**

  As this is not a vulnerability, the impact is not applicable, but it is good practice to keep everything updated and patched.

Remediation

Implement the latest Jquery libraries.

- **More Information**
  - How to upgrade to the latest version of jQuery (hubspot.com)
  - Updating jQuery Version - Stack Overflow

SECUREU

WE MAKE SECURITY ACCESSIBLE

Questions? Contact us at
Email : contact-us@secureu.in Phone : +91 8010450348