SCANCTUM Security Assessment Report **Target:**

https://mujslcm.jaipur.manipal.edu/ **Report date:** 2026-02-19 09:43 UTC **Scan mode:** Full | **Pages scanned:** 1 **Overall risk:** Critical **Confidential**

1. Executive Summary

This report presents the results of an automated vulnerability assessment performed by Scanctum. A total of **28** finding(s) were identified across **1** page(s). The overall risk level for this engagement is **Critical**. **Severity distribution**

1 Critical	4 High	14 Medium	6 Low	3 Info

OWASP Top 10 overview

Category	Description	Count
A03	Injection	1
A05	Security Misconfiguration	26
A07	Identification and Authentication Failures	1

2. Detailed Findings

OS Command Injection (Form) critical

URL `https://mujslcm.jaipur.manipal.edu/`

CVSS 9.8 (A03 / CWE-78)

Parameter EmailFor

Description Form field 'EmailFor' is vulnerable to OS command injection. **Evidence** **Payload:**

```
; echo scntm_cmd_7x9z Command Output:
...RiI1" />
```

... **Remediation** Never pass form input to shell commands. Use parameterized APIs.

Debug Endpoint Exposed high

URL `https://mujslcm.jaipur.manipal.edu/_debug/`

CVSS 7.5 (A05 / CWE-215)

Description Debug endpoint accessible at '/_debug/'. **Evidence** **Response Preview:**

JavaSc **Remediation** Block access to '/.aws/credentials' in web server configuration. Remove sensitive files from the web root.

Debug Endpoint Exposed high

URL `https://mujslcm.jaipur.manipal.edu/__debug__/`

CVSS 7.5 (A05 / CWE-215)

Description Debug endpoint accessible at '/__debug__/'. **Evidence** **Response Preview:**

JavaSc **Remediation** Block access to '/wp-config.php' in web server configuration. Remove sensitive files from the web root.

Missing Security Header: Content-Security-Policy medium

URL `https://mujslcm.jaipur.manipal.edu/`

CVSS 5.4 (A05 / CWE-16)

Description The HTTP response is missing the 'Content-Security-Policy' security header. **Evidence** **Response Headers:**

```
cache-control: private content-type: text/html; charset=utf-8 server: Microsoft-IIS/10.0
x-aspnetmvc-version: 5.3 x-frame-options: SAMEORIGIN x-aspnet-version: 4.0.30319 set-cookie:
__RequestVerificationToken=xoEJW2cA3NKKfBRVhPwokmMAwXh2xwrxUAKV3Qjp-Aw4W4A5pc_sImSasP-6uNl4IHSzWx6sXdvS-OHgpWNIt0
path=/; HttpOnly x-powered-by: ASP.NET date: Thu, 19 Feb 2026 08:15:10 GMT content-length: 20531
```

Remediation Implement a Content-Security-Policy header with appropriate directives.

Missing Security Header: Strict-Transport-Security medium

URL `https://mujslcm.jaipur.manipal.edu/`

CVSS 5.4 (A05 / CWE-523)

Description The HTTP response is missing the 'Strict-Transport-Security' security header. **Evidence** **Response Headers:**

```
cache-control: private content-type: text/html; charset=utf-8 server: Microsoft-IIS/10.0
```

`x-aspnetmvc-version: 5.3 x-frame-options: SAMEORIGIN x-aspnet-version: 4.0.30319 set-cookie: __RequestVerificationToken=xoEJW2cA3NKKfBRVhPwokmMAwXh2xwrxUAKV3Qjp-Aw4W4A5pc_sImSasP-6uNl4IHSzWx6sXdvS-OHgpWNIt0 path=/; HttpOnly x-powered-by: ASP.NET date: Thu, 19 Feb 2026 08:15:10 GMT content-length: 20531`

Remediation Add 'Strict-Transport-Security: max-age=31536000; includeSubDomains' header. **Exposed Sensitive File: Debug Endpoint** medium

URL `https://mujslcm.jaipur.manipal.edu/debug/`

CVSS 5.3 (A05 / CWE-538)

Description Sensitive file '/debug/' is publicly accessible. **Evidence** **`Response Preview:`**

Remediation Block access to '/debug/' in web server configuration. Remove sensitive files from the web root. **Missing Rate Limiting on Authentication** medium

URL `https://mujslcm.jaipur.manipal.edu/`

CVSS 5.3 (A07 / CWE-307)

Description No rate limiting headers detected on a page with authentication form. This could allow brute-force attacks. **Evidence** **`Response Headers (no rate limit headers found):`**

`cache-control: private content-type: text/html; charset=utf-8 server: Microsoft-IIS/10.0 x-aspnetmvc-version: 5.3 x-frame-options: SAMEORIGIN x-aspnet-version: 4.0.30319 x-powered-by: ASP.NET date: Thu, 19 Feb 2026 08:16:15 GMT content-length: 20531` **Remediation** Implement rate limiting on authentication endpoints. Add progressive delays and account lockout policies. **Exposed Sensitive File: Apache Configuration** medium

URL `https://mujslcm.jaipur.manipal.edu/.htaccess`

CVSS 5.3 (A05 / CWE-538)

Description Sensitive file '/.htaccess' is publicly accessible. **Evidence** **`Response Preview:`**

Remediation Block access to '/.htaccess' in web server configuration. Remove sensitive files from the web root. **Exposed Sensitive File: Node.js Package Manifest** medium

URL `https://mujslcm.jaipur.manipal.edu/package.json`

CVSS 5.3 (A05 / CWE-538)

Description Sensitive file '/package.json' is publicly accessible. **Evidence** **`Response Preview:`**

Remediation Block access to '/package.json' in web server configuration. Remove sensitive files from the web root. **Exposed Sensitive File: PHP Composer Manifest** medium

URL `https://mujslcm.jaipur.manipal.edu/composer.json`

CVSS 5.3 (A05 / CWE-538)

Description Sensitive file '/composer.json' is publicly accessible. **Evidence** **`Response Preview:`**

Remediation Block access to '/composer.json' in web server configuration. Remove sensitive files from the web root. **Exposed Sensitive File: Ruby Gemfile** medium

URL `https://mujslcm.jaipur.manipal.edu/Gemfile`

CVSS 5.3 (A05 / CWE-538)

Description Sensitive file '/Gemfile' is publicly accessible. **Evidence** **`Response Preview:`**

Remediation Block access to '/Gemfile' in web server configuration. Remove sensitive files from the web root. **Exposed Sensitive File: Docker Environment** medium

URL `https://mujslcm.jaipur.manipal.edu/.dockerenv`

CVSS 5.3 (A05 / CWE-538)

Description Sensitive file '/.dockerenv' is publicly accessible. **Evidence** **`Response Preview:`**

Remediation Block access to '/.dockerenv' in web server configuration. Remove sensitive files from the web root. **Exposed Sensitive File: Docker Compose File** medium

URL `https://mujslcm.jaipur.manipal.edu/docker-compose.yml`

CVSS 5.3 (A05 / CWE-538)

Description Sensitive file '/docker-compose.yml' is publicly accessible. **Evidence** **`Response Preview:`**

Remediation Block access to '/docker-compose.yml' in web server configuration. Remove

sensitive files from the web root. **Exposed Sensitive File: macOS Directory Store** medium

URL `https://mujslcm.jaipur.manipal.edu/.DS_Store`

CVSS 5.3 (A05 / CWE-538)

Description Sensitive file '/.DS_Store' is publicly accessible. **Evidence** **Response Preview:**

Remediation Block access to '/.DS_Store' in web server configuration. Remove sensitive files from the web root. **Exposed Sensitive File: Flash Cross-Domain Policy** medium

URL `https://mujslcm.jaipur.manipal.edu/crossdomain.xml`

CVSS 5.3 (A05 / CWE-538)

Description Sensitive file '/crossdomain.xml' is publicly accessible. **Evidence** **Response Preview:**

Remediation Block access to '/crossdomain.xml' in web server configuration. Remove sensitive files from the web root. **Exposed Sensitive File: Sitemap (Info Disclosure)** medium

URL `https://mujslcm.jaipur.manipal.edu/sitemap.xml`

CVSS 5.3 (A05 / CWE-538)

Description Sensitive file '/sitemap.xml' is publicly accessible. **Evidence** **Response Preview:**

Remediation Block access to '/sitemap.xml' in web server configuration. Remove sensitive files from the web root. **Exposed Sensitive File: PHP Configuration** medium

URL `https://mujslcm.jaipur.manipal.edu/config.php`

CVSS 5.3 (A05 / CWE-538)

Description Sensitive file '/config.php' is publicly accessible. **Evidence** **Response Preview:**

Remediation Block access to '/config.php' in web server configuration. Remove sensitive files from the web root. **Missing Security Header: X-XSS-Protection** low

URL `https://mujslcm.jaipur.manipal.edu/`

CVSS 3.1 (A05 / CWE-16)

Description The HTTP response is missing the 'X-XSS-Protection' security header. **Evidence** **Response Headers:**

```
cache-control: private content-type: text/html; charset=utf-8 server: Microsoft-IIS/10.0
x-aspnetmvc-version: 5.3 x-frame-options: SAMEORIGIN x-aspnet-version: 4.0.30319 set-cookie:
__RequestVerificationToken=xoEJW2cA3NKKfBRVhPwokmMAwXh2xwrxUAKV3Qjp-Aw4W4A5pc_sImSasP-6uNl4IHSzWx6sXdvS-OHgpWNIt0
path=/; HttpOnly x-powered-by: ASP.NET date: Thu, 19 Feb 2026 08:15:10 GMT content-length: 20531
```

Remediation Add 'X-XSS-Protection: 1; mode=block' header (or rely on CSP). **Missing Security Header: Referrer-Policy** low

URL `https://mujslcm.jaipur.manipal.edu/`

CVSS 3.1 (A05 / CWE-116)

Description The HTTP response is missing the 'Referrer-Policy' security header. **Evidence** **Response Headers:**

```
cache-control: private content-type: text/html; charset=utf-8 server: Microsoft-IIS/10.0
x-aspnetmvc-version: 5.3 x-frame-options: SAMEORIGIN x-aspnet-version: 4.0.30319 set-cookie:
__RequestVerificationToken=xoEJW2cA3NKKfBRVhPwokmMAwXh2xwrxUAKV3Qjp-Aw4W4A5pc_sImSasP-6uNl4IHSzWx6sXdvS-OHgpWNIt0
path=/; HttpOnly x-powered-by: ASP.NET date: Thu, 19 Feb 2026 08:15:10 GMT content-length: 20531
```

Remediation Add 'Referrer-Policy: strict-origin-when-cross-origin' header. **Missing Security Header: Permissions-Policy** low

URL `https://mujslcm.jaipur.manipal.edu/`

CVSS 3.1 (A05 / CWE-16)

Description The HTTP response is missing the 'Permissions-Policy' security header. **Evidence** **Response Headers:**

```
cache-control: private content-type: text/html; charset=utf-8 server: Microsoft-IIS/10.0
x-aspnetmvc-version: 5.3 x-frame-options: SAMEORIGIN x-aspnet-version: 4.0.30319 set-cookie:
__RequestVerificationToken=xoEJW2cA3NKKfBRVhPwokmMAwXh2xwrxUAKV3Qjp-Aw4W4A5pc_sImSasP-6uNl4IHSzWx6sXdvS-OHgpWNIt0
path=/; HttpOnly x-powered-by: ASP.NET date: Thu, 19 Feb 2026 08:15:10 GMT content-length: 20531
```

Remediation Add Permissions-Policy header to control browser features. **Missing Security Header: X-Content-Type-Options** low

URL https://mujslcm.jaipur.manipal.edu/

CVSS 3.1 (A05 / CWE-16)

Description The HTTP response is missing the 'X-Content-Type-Options' security header. **Evidence** **Response Headers:**

```
cache-control: private content-type: text/html; charset=utf-8 server: Microsoft-IIS/10.0
x-aspnetmvc-version: 5.3 x-frame-options: SAMEORIGIN x-aspnet-version: 4.0.30319 set-cookie:
__RequestVerificationToken=xoEJW2cA3NKKfBRVhPwokmMAwXh2xwrxUAKV3Qjp-Aw4W4A5pc_sImSasP-6uNl4IHSzWx6sXdvS-OHgpWNIt0
path=/; HttpOnly x-powered-by: ASP.NET date: Thu, 19 Feb 2026 08:15:10 GMT content-length: 20531
```

Remediation Add 'X-Content-Type-Options: nosniff' header. **Cookie Missing Secure Flag** low

URL https://mujslcm.jaipur.manipal.edu/

CVSS 3.1 (A05 / CWE-614)

Parameter __RequestVerificationToken

Description Cookie '__RequestVerificationToken' is missing the Secure flag, allowing transmission over HTTP. **Evidence** **Set-Cookie Header:**

```
__RequestVerificationToken=xoEJW2cA3NKKfBRVhPwokmMAwXh2xwrxUAKV3Qjp-Aw4W4A5pc_sImSasP-6uNl4IHSzWx6sXdvS-OHgpWNIt0
path=/; HttpOnly
```

Remediation Add the Secure flag so the cookie is only sent over HTTPS. **Cookie Missing SameSite Attribute** low

URL https://mujslcm.jaipur.manipal.edu/

CVSS 3.1 (A05 / CWE-1275)

Parameter __RequestVerificationToken

Description Cookie '__RequestVerificationToken' is missing the SameSite attribute. **Evidence** **Set-Cookie Header:**

```
__RequestVerificationToken=xoEJW2cA3NKKfBRVhPwokmMAwXh2xwrxUAKV3Qjp-Aw4W4A5pc_sImSasP-6uNl4IHSzWx6sXdvS-OHgpWNIt0
path=/; HttpOnly
```

Remediation Add 'SameSite=Lax' or 'SameSite=Strict' attribute. **Information Disclosure: Server Header** info

URL https://mujslcm.jaipur.manipal.edu/

CVSS 0.0 (A05 / CWE-200)

Description The 'Server' header discloses server information: Microsoft-IIS/10.0 **Evidence** **Server Value:**

```
Server: Microsoft-IIS/10.0
```

Remediation Remove or suppress the 'Server' header in production. **Information Disclosure: X-Powered-By Header** info

URL https://mujslcm.jaipur.manipal.edu/

CVSS 0.0 (A05 / CWE-200)

Description The 'X-Powered-By' header discloses server information: ASP.NET **Evidence** **X-Powered-By Value:**

```
X-Powered-By: ASP.NET
```

Remediation Remove or suppress the 'X-Powered-By' header in production.

Information Disclosure: X-AspNet-Version Header info

URL https://mujslcm.jaipur.manipal.edu/

CVSS 0.0 (A05 / CWE-200)

Description The 'X-AspNet-Version' header discloses server information: 4.0.30319 **Evidence** **X-AspNet-Version Value:**

```
X-AspNet-Version: 4.0.30319
```

Remediation Remove or suppress the 'X-AspNet-Version' header in production.

3. Disclaimer