NCST QA Environment – Security Validation Report

Assessment Details

Item	Details
Application	NCST Portal
Environment	QA
Target URL	https://ncst-qa.dhanushinfotech.com
Web Server	Nginx Reverse Proxy
WAF Solution	ModSecurity
OWASP CRS Version	4.27.0
Assessment Date	29-Jun-2026
Assessed By	Sateesh Perala

Objective

To validate the security controls implemented on the NCST QA environment and verify that the Nginx Reverse Proxy integrated with ModSecurity and OWASP Core Rule Set (CRS) is capable of detecting and blocking common web application attacks.

Scope of Testing

Security validation was performed against:

Target URL: https://ncst-qa.dhanushinfotech.com

Validation Activities Performed

- Security Header Verification
- TLS/SSL Configuration Validation
- HTTP Method Restriction Testing
- Information Disclosure Checks
- ModSecurity Verification
- OWASP CRS Rule Validation
- Attack Simulation Testing
- Audit Log Verification

Tools Used

- curl
- OpenSSL
- Linux Command-Line Utilities
- ModSecurity Audit Logs
- Nginx Logs

Security Hardening Verification

Security Control	Status
HTTPS Enabled	PASS
TLS 1.0 Disabled	PASS
TLS 1.1 Disabled	PASS
TLS 1.2 Enabled	PASS
TLS 1.3 Enabled	PASS
HSTS Enabled	PASS
Content Security Policy (CSP)	PASS
X-Frame-Options	PASS
X-Content-Type-Options	PASS
Permissions-Policy	PASS
Server Banner Hidden	PASS
Directory Listing Disabled	PASS
Sensitive File Access Protected	PASS
TRACE Method Disabled	PASS
PUT Method Restricted	PASS
DELETE Method Restricted	PASS

ModSecurity & OWASP CRS Verification

The following components were verified:

- ModSecurity Engine Enabled
- OWASP CRS 4.27.0 Loaded

- Blocking Mode Enabled
- Audit Logging Enabled
- Anomaly Scoring Enabled
- Inbound Anomaly Threshold Configured

Status: PASS

Attack Simulation Results

Attack Category	Result	Status
Local File Inclusion (LFI)	Blocked (HTTP 403)	PASS
Path Traversal	Blocked (HTTP 403)	PASS
Cross Site Scripting (XSS)	Blocked (HTTP 403)	PASS
SQL Injection (SQLi)	Blocked (HTTP 403)	PASS
Remote Command Execution (RCE)	Blocked (HTTP 403)	PASS
PHP Injection	Detected and Blocked	PASS

Key OWASP CRS Rules Triggered During Validation

Rule ID	Description
930130	Restricted File Access Attempt
932160	Command Execution / File Access Detection
933135	PHP Injection Detection
941100	XSS Attack Detection
942100	SQL Injection Detection
949110	Inbound Anomaly Score Blocking

Audit Log Validation

ModSecurity audit logs were reviewed to verify:

- Attack detection
- Rule execution
- Anomaly score calculation
- Automatic request blocking

The logs confirmed that malicious requests were successfully detected and blocked by the configured OWASP CRS rules.

Status: PASS

Conclusion

Security validation testing was successfully completed against the QA environment hosted at:

https://ncst-qa.dhanushinfotech.com

The implemented Nginx Reverse Proxy, ModSecurity, and OWASP CRS 4.27.0 configuration successfully detected and blocked all tested attack vectors, including XSS, SQL Injection, Path Traversal, Local File Inclusion, Remote Command Execution, and PHP Injection attempts.

Security hardening controls such as TLS configuration, security headers, HTTP method restrictions, information disclosure protection, and audit logging were also verified successfully.

Final Result

Overall Security Validation Status: PASS

Recommendation

The current QA deployment has successfully passed the security validation checks performed on the Nginx WAF layer and is suitable for further QA/UAT testing.