OPSWAT UNIT 515 PEN TESTING SERVICES

Pen Testing Report for {Customer} - {Enterprise Application}

Prepared for **[Logo]**

01
Executive Summary

OPSWAT Unit 515 pen testing delivers targeted security assessments for enterprise applications that simulate real-world web attacks to expose vulnerabilities in public-facing, internal web applications, APIs, and admin dashboards.

This service focuses on the detailed analysis of security risks across:

- Web Application Security Assessment
- API Security Testing
- Portal Authentication & Session Management Testing
- Secure File Upload Testing
- Injection Vulnerability Testing
- Role-Based Access Control Bypass Testing
- Admin Panel Exposure and Exploitation

Unit 515's extensive OT and IT security expertise helps organizations uncover vulnerabilities, assess risks, and mitigate threats. Our penetration testing service provides clear insight into business impact and equips teams with actionable steps to strengthen their security posture.

Client Name	Customer Name
Client technical Contact	Customer@companyemail.com
Client Executive Sponsor	Customer@companyemail.com
Project Name	OPSWAT Penetration testing Report of Enterprise application
Document Date / Version	22/05/2025 – 1.0.0

Table of Contents

02.
Key Findings Overview

Following an extensive penetration testing procedure encompassing all the components of the targeted enterprise application, a total of 7 security vulnerabilities were identified. These vulnerabilities comprised **01** critical, **01** high, **01** medium, **03** low, and **01** information-level security issues.

Severity	Critical	High	Medium	Low	Information
Count	1	1	1	3	1

Total number of findings with correlation of Severity against Business Impact:

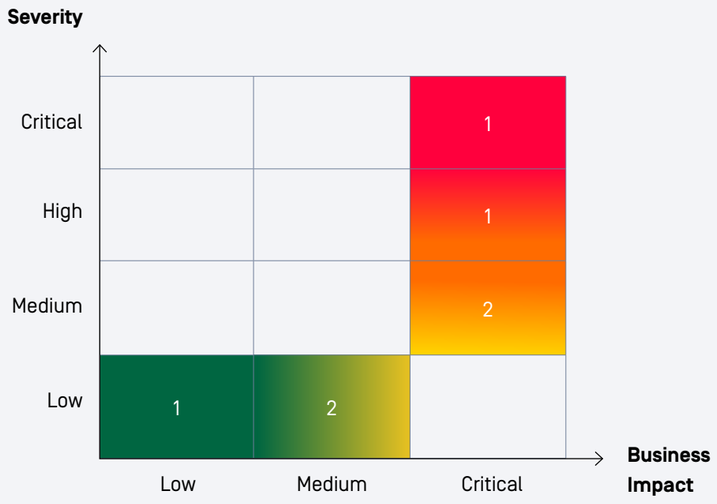


Figure 2: Correlation of Findings considering business impact against severity level

03.
Business Impact Summary

Below is an example of the Test Findings, where the table displays the detailed security findings classified by severity, providing specific insights into each category of vulnerability:

Sno	Security Findings	Severity	Score	Business Impact
1	Authentication Bypass via SAML	Critical	9,8	Critical
2	Remote Code Execution via Application workflow Feature	High	7,2	Critical
3	Sensitive Data Disclosure in Audit Log	Medium	6,5	Critical
4	HTML Injection	Low	3,5	Medium
5	CSV Injection	Low	2,6	Medium
6	Improper Log Handling	Low	2,6	Low
8	Improper Error Response Handling	Information	N/A	None

04.
Application Scope

As an initial step, we have identified the utilization of the following specific technologies:

Feature	Technique
Targeted Enterprise Application – V1.0.0 ▪ Web Management Console & REST API ▪ Hosted On Premise	▪ Microservices (API) ▪ Nginx ▪ Angular ▪ SQLite ▪ DotNET

05. Detailed Security Risk Report & Remediation

This sample report highlights the security findings from the penetration testing. It details the description, impact, and arrived risk score, along with proof of exploit, business impact, and remediation steps for critical and high vulnerabilities.

5.1. Authentication Bypass via SAML

Critical Vulnerability – Authentication Bypass via SAML	
Description	Targeted Enterprise application Security supports SAML authentication, but the application fails to properly validate the signature in the SAM Response when it is generated with a fake private key or omitted entirely. Consequently, the attacker can forge or omit the signature with tampered data to gain access as a high-privileged user.
Impact	The unauthenticated attacker can gain access as a high-privileged user in Targeted Enterprise application.
CVSS Score	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Affected Endpoint	[POST] - /XXXXXXX /saml/{id}

Proof of Exploit

- Target Enterprise Application fails to properly validate the signature in the SAMLResponse when it is generated using a fake private key or omitted entirely.
- The documented artifacts capture differences between a valid SAMLResponse and a malicious SAMLResponse that lacks a signature and contains tampered data.
- The application still accepts the SAMLResponse above and issues cookies.
- Consequently, a malicious user can forge or omit the signature with tampered data, gaining high-privileged access without authorization; or an unauthenticated user can brute force the Login Callback URL and use it to craft a valid signature, gaining access to Targeted Enterprise Application without any credentials.
- **Artifacts related to proof of exploit are shared in a detailed report separately for confidentiality.**
- **Attached sample artifact for evidence of proof of exploit.**

Business Impact of the Security Finding

Unauthenticated attackers can gain access to elevated privilege of the system and perform admin level activities that can result in modification of the administrator rules and can add users outside the organization scope to allow unauthorized access to the system.

Remediation

- Validate the signature of the SAML response with the public key of the IdP instead of the public key attached to the response.
- Use third party library for SAML authentication.

References

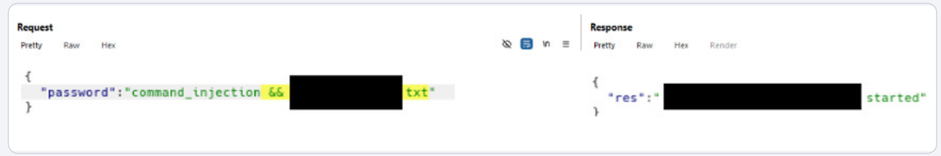
SAML Security - OWASP Cheat Sheet Series

5.2. Security Finding Details - Remote Code Execution via Application Workflow Feature

High Vulnerability - Remote Code Execution via Application Workflow Feature	
Description	Targeted enterprise application security support application features are managed through packages, password protected, and passed through the command line. This finding highlights the risk of command line injection attack.
Impact	This vulnerability allows attackers to execute arbitrary commands during the package generation process. Since the process runs with elevated privileges, this could lead to a remote code execution attack, granting full control over the system.
CVSS Score	7.2 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N
Affected Endpoint	[POST] - /XXXXXXX /workflow/package

Proof of Exploit

- Target Enterprise Application fails to properly validate the password generated during the package creation for the application workflow.
- The documented artifacts capture creation of the package and executing an OS command line injection attack with generated password.
- The application still accepts non validated /sanitized password parameters
- Consequently, a malicious user can inject malicious code while calling the password and enabling the execution of the injected code and thus compromising the enterprise application server.
- **Artifacts related to proof of exploit are shared in detailed report separately for confidentiality.**
- **Attached sample artifact for evidence of proof of exploit.**



Business Impact of the Security Finding

Attackers can gain access to elevated privileges and perform remote code execution that can result in unauthorized access to the system.

Remediation

Validate the password values and escape any special characters (such as ;, &, |, $, etc.) that could be interpreted as command separators or operators

References

OS Command Injection Defense - OWASP Cheat Sheet Series

06.
Concluding Assessment

These security vulnerabilities have the potential to cause significant impacts, including:

- If SAML authentication is enabled, an unauthenticated attacker could bypass secure authentication in the targeted enterprise application and gain administrator-level access to the Web Management Console.
- A malicious attacker could exploit the application workflow feature to execute harmful commands and compromise the Messaging feature functionality.

Targeted enterprise application owner to incorporate remediation efforts outlined in the security findings report into application development practices and re-assess the non-occurrence of the security risk.

Remediation for each security finding can be identified in the following sections of this report:

07.
Appendix: Risk Rating Scoring Factors

Attack Vector (AV)	Describes how the vulnerability can be exploited.
Attack Complexity (AC)	Reflects the level of expertise required to exploit the vulnerability.
Privileges Required (PR)	Indicates the privileges an attacker must possess to exploit the vulnerability.
User Interaction (UI)	Reflects whether user interaction is required for exploitation.
Scope (S)	Defines the extent of the impact if the vulnerability is exploited.
Confidentiality (C), Integrity (I), and Availability (A)	Rate the impact on these three core security principles.
Exploit Code Maturity (E)	Reflects the maturity level of known exploits.
Remediation Level (RL)	Describes the availability and maturity of remediations.
Report Confidence (RC)	Reflects the level of confidence in the vulnerability details.

We assign risk ratings based on the CVSS Base Score as follows:

Severity	Base Score
Critical	>= 9.0
High	>= 7.0 and < 9.0
Medium	>= 4.0 and < 7.0
Low	< 4.0
Information	N/A

Severity level classification based on CVSS Risk Scoring.

GET STARTED

Let’s close these gaps and prevent attacks.

Talk to one of our experts today.

Scan the QR code or send us an email at:
pentest@opswat.com

OPSWAT.

Proactive security starts here.

To strengthen your security posture, we recommend addressing the identified vulnerabilities using the remediation guidance in this report and scheduling a follow-up assessment with Unit 515 to verify closure and reduce your risk exposure.

Unit 515 is OPSWAT’s elite red team, specializing in proactive web application security through adversary simulation.

©2025 OPSWAT Inc. All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.