PENETRATION TESTING REPORT
FOR
def

PT Conducted on Feb 2026

Conducted by abc

Document Type	Penetration Testing Report	Version	1.0
Assessee	def	Signature	
Assessor	abc	Signature	
Reviewer	Jane	Signature	
Approved by	CTO	Signature	

Table of Contents

Scan Manifest		
a.	Description	Web Application Penetration Testing
b.	Test started on	25-Feb-2026
c.	Test Completed on	26-Feb-2026
d.	No. of URL’s tested	1 URL
e.	Standard / Test Procedure reference	OWASP TOP 10, SANS 25
f.	Test performed at	Off-site
g.	Tool used for testing	Burp Suite, Open-Source Tools

1. Executive Summary

1.1 Overview

A security assessment was conducted to evaluate the effectiveness of existing controls and to identify vulnerabilities that may impact the confidentiality, integrity, and availability of the assessed environment.

The engagement was performed using industry-recognized testing methodologies and simulated real-world attack scenarios to assess potential exposure to security threats. The objective was to identify exploitable weaknesses that could result in unauthorized access, data compromise, privilege escalation, or service disruption.

The assessment identified findings across multiple severity levels. Each observation has been risk-rated based on standardized classification criteria and includes detailed technical analysis, impact evaluation, and recommended remediation measures.

Timely remediation of identified high-risk vulnerabilities is recommended to reduce overall exposure and strengthen the organization's security posture.

1.2 Risk Model

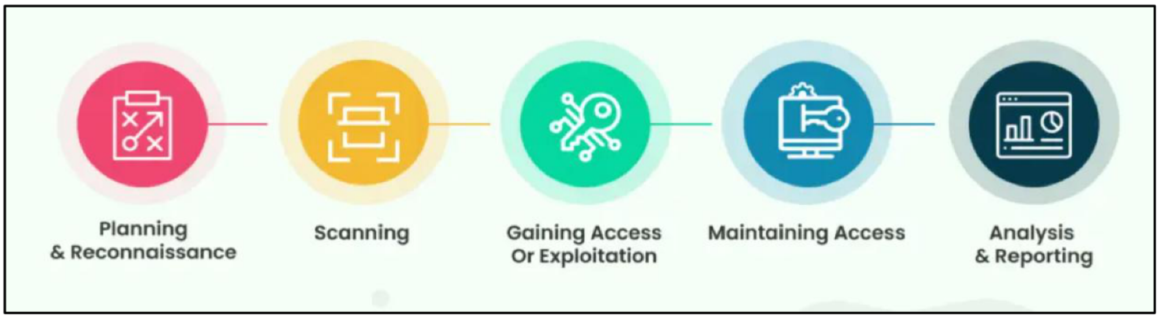
Throughout this document, **abc** has categorized the risk ratings for discovered vulnerabilities based on global standard risk definitions.

Priority Level	Severity Scale	CVSS Score	Description of Vulnerability
P1	Critical	9.0 – 10.0	The exposure may be exploited resulting in bad outcomes such as unauthorized privilege escalation, data access, downtime, or compromise of data.
P2	High	7.0 – 8.9	These issues identify conditions that could directly result in the compromise or unauthorized access of a network, system, application, or sensitive information.
P3	Medium	4.0 – 6.9	These issues identify conditions that do not immediately or directly result in the compromise or unauthorized access of a network, system, application, or sensitive information, but do provide a capability or information that could in combination with others' capabilities or information result in the compromise unauthorized access of a network application or information.
P4	Low	0.1 – 3.9	These issues identify conditions that do not immediately or directly result in the compromise of a network, system, application, or information but do provide information that could be used in combination with others' information that could be used in combination with other's information access to a network system,application,or information.
P5	Informational	0	Issues that leaking very basic information which might lead to information disclosure.

2. Web Application Penetration Testing Methodology

- **Information Gathering**
- **Enumeration**
- **Scanning**
- **Exploitation**
- **Reporting**

The following also gives a high-level description and process of Security Analysts methodology used for performing the Web application testing:



1. Planning and Reconnaissance
In this initial phase, the scope and objectives of the penetration test are defined. The tester gathers relevant information about the target system through documentation review and publicly available sources to understand the environment.

2. Scanning
The tester uses automated and manual tools to identify vulnerabilities such as open ports, weak credentials, and misconfigurations. This phase helps determine potential entry points for exploitation.

3. Gaining Access
The identified vulnerabilities are exploited to gain unauthorized access. Techniques may include SQL injection, password attacks, or social engineering, depending on the defined scope.

4. Maintaining Access (Optional)
If permitted, the tester attempts to establish persistence within the compromised system. This phase evaluates lateral movement, privilege escalation, and the overall impact of sustained unauthorized access.

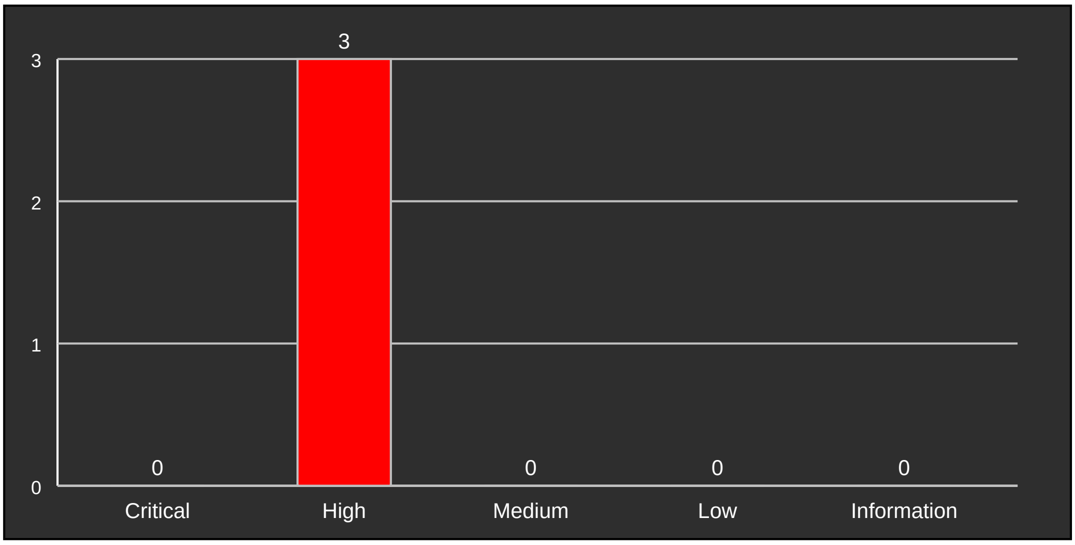
5. Reporting
After completing the assessment, a detailed report is prepared outlining the vulnerabilities identified, their risk level, and potential business impact. The report also provides clear and prioritized remediation recommendations.

3. Project Scope

Formal communication from the def outlined the application to be tested and the type of testing to be carried out. A RED team resource was deployed to perform this activity.

4. Penetration Testing Results

URL	Critical	High	Medium	Low	Information
https://def	**0**	**3**	**0**	**0**	**0**



S.No	Vulnerability Name	Severity	Status
1	Access another user’s data via IDOR	HIGH	Pending
2	Access admin panel without authorization	HIGH	Pending
3	Force browsing to restricted URLs	HIGH	Pending

3. Detailed Findings

Vulnerability 1	Access another user’s data via IDOR
Severity	**HIGH**
Description	By modifying object identifiers in requests, users can access data belonging to other users. The application does not validate ownership of the requested objects.
Impact	Exposure of sensitive user data Violation of user privacy Potential regulatory and compliance issues
Recommendation	Validate object ownership on the server Avoid exposing direct object identifiers Enforce authorization checks for each request

Vulnerability 2	Access admin panel without authorization
Severity	**HIGH**
Description	The application allows access to administrative endpoints without validating the user’s authorization level. Requests made by low-privileged users are processed successfully without server-side permission checks.
Impact	Unauthorized access to administrative functionality Modification or exposure of sensitive system data Complete compromise of application security
Recommendation	Implement strict server-side authorization checks Validate user roles before granting access to admin endpoints Restrict administrative functionality to privileged users only

Vulnerability 3	Force browsing to restricted URLs
Severity	**HIGH**
Description	Restricted URLs can be accessed directly by entering them in the browser without proper authorization checks. The application does not enforce access control on these endpoints.
Impact	Exposure of restricted application functionality Unauthorized access to sensitive resources Bypass of intended access restrictions
Recommendation	Apply authorization checks to all restricted URLs Deny direct access to sensitive endpoints Implement centralized access control rules

5. Conclusion

Nevertheless, we suggest that the application allocated to def implement the recommendations in this document with respect to the affected application. We also propose to follow-on retest to verify that the recommended changes were made and made correctly. Please note that as technologies and risks change over time, the vulnerabilities associated with the operation of the applications described in this report, as well as the actions necessary to reduce the exposure to such vulnerabilities, will also change.

----END OF THE DOCUMENT----