Web Application Penetration Test Report

Client: [Client Name]

Assessment Type: Web Application Penetration Test

Test Dates: [Start Date] – [End Date]

Prepared By: Deepak Rawat

Version: 1.0

Confidential

# Table of Contents

1. Executive Summary

2. Scope & Objectives

3. Methodology

4. Vulnerability Risk Ratings

5. Summary of Findings

6. Technical Details

7. Recommendations

8. Appendices

# 1. Executive Summary

This assessment focused on identifying vulnerabilities in the web application hosted at [application URL]. The test simulated real-world attack scenarios using OWASP Top 10, NIST 800-115, and custom threat modeling.  
  
Highlights:  
- Total Findings: 12  
- Critical: 2 | High: 3 | Medium: 4 | Low: 2 | Info: 1  
- Domain admin or data breach risk: ❌ Not achieved

# 2. Scope & Objectives

- In-scope URL: https://app.client.com  
- Authenticated areas: Yes  
- Out-of-scope: admin.client.com, DoS, Social Engineering

# 3. Methodology

- Reconnaissance & Mapping  
- Authentication Testing  
- Business Logic Testing  
- Input Validation Testing  
- Authorization Checks  
- Exploitation & Proof-of-Concept  
- Reporting

# 4. Vulnerability Risk Ratings

|  |  |  |
| --- | --- | --- |
| Severity | CVSS Score | Description |
| Critical | 9.0–10.0 | Remote code exec, auth bypass |
| High | 7.0–8.9 | Privilege escalation, data leak |
| Medium | 4.0–6.9 | Auth issues, injections |
| Low | 0.1–3.9 | Info disclosure, minor misconfigs |
| Info | N/A | No risk, informative only |

# 6. Technical Details - Sample Finding

ID: WEB-001  
Title: SQL Injection in 'search' parameter  
Severity: Critical  
Description: The 'search' parameter on the /products endpoint is vulnerable to SQL injection. A crafted payload resulted in database error messages and confirmed data exfiltration.  
Recommendation: Implement parameterized queries and input validation.  
Proof of Concept: ' OR '1'='1 --