CONFIDENTIAL - SECURITY ASSESSMENT REPORT

Penetration Testing Report for 10root

Report Date: May 14, 2025

Assessment Period: April 23 - May 7, 2025

Report Version: 1.0

Classification: CONFIDENTIAL

1. Executive Summary

This report presents the findings of a comprehensive penetration test conducted on 10root's IT infrastructure and applications. The assessment identified several critical and high-risk vulnerabilities that could potentially expose sensitive customer data and business information to unauthorized access.

10root (https://www.10root.com) requested this penetration test to evaluate their security posture prior to launching their new cloud security platform. Our team conducted external and internal network testing, web application assessments, and social engineering tests.

2. Company Information

Client Details:

- Company Name: 10root, Inc.
- Primary Domain: 10root.com
- IP Range: 198.51.100.0/24
- Main Office: 1234 Cyber Street, Suite 567, San Francisco, CA 94105

- Data Center: 5678 Server Lane, Santa Clara, CA 95051

Key Contacts:

- Sarah Johnson, CTO (sarah.johnson@10root.com, +1-415-555-7890)
- Michael Chen, CISO (michael.chen@10root.com, +1-415-555-1234)
- Security Operations Center (soc@10root.com, +1-415-555-9876)
- IT Support (support@10root.com, +1-415-555-4321)
- Emergency Contact (emergency@10root.com, +1-415-555-0911)

3. Assessment Scope

The penetration test included the following:

- External network (198.51.100.0/24)
- Web applications:
  - https://www.10root.com
  - https://portal.10root.com
  - https://api.10root.com
  - https://admin.10root.com
  - https://support.10root.com
- Internal network (10.10.0.0/16)
- AWS cloud infrastructure (account ID: 012345678901)
- Social engineering assessment

4. High-Risk Findings

4.1. Exposed API Credentials (Critical)

Found in GitHub repo 10root/cloud-scanner. Exposed keys linked to David Wilson (david.wilson@10root.com).

4.2. Vulnerable Authentication in Customer Portal (Critical)

Session fixation vulnerability at https://portal.10root.com.

4.3. SQL Injection in API Endpoint (High)

Vulnerability at https://api.10root.com/v1/customers/search.

5. Medium-Risk Findings

5.1. Insecure Direct Object References (Medium)

Affects https://support.10root.com endpoints.

5.2. Missing MFA for Admin Access (Medium)

Admin accounts without MFA include:

- John Adams, Elena Rodriguez, Terry Zhang, Alex Washington

5.3. Sensitive Data Stored on Public S3 Bucket (Medium)

Public bucket: s3://10root-customer-backup/

6. Additional Findings

- DNS version info exposed
- Outdated Apache version on legacy.10root.com
- Unencrypted internal communication
- Weak password policy

7. Recommendations

1. Rotate exposed AWS keys
2. Secure session management
3. Validate input and parameterize queries
4. Enforce authorization checks
5. Enable MFA for all admins
6. Secure S3 buckets

8. Conclusion

Significant security improvements needed. Critical risks should be addressed immediately.

9. Appendices

9.1. Team Members

- Daniel Brown, Jennifer Lee, Mark Williams, Rachel Green

9.2. Testing Methodology

Based on OWASP and NIST SP 800-115.

CONFIDENTIAL - DO NOT DISTRIBUTE