Analyst #: 6579

Pequity Pentest Summary Report

Pequity

August, 2021

Table of Contents

1 Executive Summary

Pequity has engaged BSK Consulting LLC to provide a penetration test against its internal and internet-facing information technology infrastructure. Testing was performed remotely via internet in testing environment. Finding categories, severities, and CVSS scores are aligned with Pequity standards.

BSK Consulting LLC performed retesting on 8/27/21, and confirmed all issues, identified in the report, have been remediated.

Targets Overview

During the discovery phase of this assessment 1 host exposing 2 services were found.

Findings Overview

Throughout auditing, 7 issues were found in 1 instance, resulting in 7 vulnerabilities in total.

About BSK Security

BSK Security LLC is a boutique security firm specializing in penetration testing. Team members are industry certified by the SANS organization. For extra information or to get in touch please contact us through our website: bsk-security.com.

2 Appendix – Methodology Overview

Application vulnerability testing, equivalent of a dynamic application security and comprehensive manual penetration testing, will evaluate the application for standard and advanced application web security issues, including but not limited to:

a. Security scanning will evaluate the application for standard application web security issues, equivalent of a WebInspect OWASP Top10 dynamic scan, including but not limited to:
    i. Determine if insecure methods are enabled.
    ii. Cross-site scripting ("XSS").
    iii. Cross-Site Request Forgery ("CSRF").
    iv. Vulnerabilities in rich content (e.g. Flash, ActiveX, Silverlight).
    v. Command injection (Structured Query Language ("SQL"), Lightweight Directory Access Protocol ("LDAP"), and Operating System ("OS") command injection.
    vi. Server-Side Includes ("SSI") injection.
    vii. Common weaknesses in session management (authentication and authorization) including:
        1. Improper token invalidation.
        2. Predictable session tokens.
        3. Insufficient protection against session fixation.
    ii. Cookie injection attacks.
    iii. Extensible Markup Language ("XML") injection attacks.
    iv. Attempt to access server information without SSL.
    v. Attempt to obtain session IDs.
    vi. Attacks against the HTTP application server, including:
        1. Insecure configuration.
        2. Processing of unsafe HTTP verbs.
        3. Response splitting.
        4. Directory traversal.
        5. Forced browsing.
    vii. Information leaks.
    viii. Transport layer security weaknesses, including:
        1. Weak cipher suite configuration.
        2. Insufficient protection of sensitive information in transit.
b. Validate false positives findings from the scan based on Pequity approved guidelines for exceptions.
c. Time boxed manual penetration testing which covers and is not limited to:
    i. Obtain access to applications private data belonging to other user or subscriber accounts/credentials
    ii. Make unauthorized changes to system or customer data.
    iii. Bypass business logic rules around account changes.
    iv. Bypass authentication and authorization mechanisms.
    v. Unvalidated Redirects for forwards.
    vi. Elevate user privileges to site administrator or other higher-privileged users.
    vii. Determine information about customer Internet Protocol address.
    viii. Access servers using false credentials.
    ix. Directly access files on servers not intended to be exposed to customers.
    x. Hijack accounts belonging to other users.
    xi. Abuse username and password recovery methods, e.g. validate if an attacker can use password recovery methods to gain access to valid user login credential.