ECHELON
RISK +
CYBER

WEB APPLICATION PENETRATION TEST

PREPARED FOR

PEQUITY

APRIL 28, 2025

CONTENTS

EXECUTIVE SUMMARY

Summary

Pequity engaged Echelon Risk + Cyber (Echelon) to perform a web application penetration test and vulnerability scan against Pequity's staging environment. Echelon identified one medium-risk vulnerability within the application that involves the potential for account compromise with unlimited password guess attempts.

Pequity engaged Echelon Risk + Cyber (Echelon) to perform a web application penetration test and vulnerability scan against Pequity's staging environment. Echelon identified one medium-risk vulnerability within the application that involves the potential for account compromise with unlimited password guess attempts. Common attack vectors such as injection attempts, client-side attacks, and other typical web application vulnerabilities were thoroughly tested. No significant exploitable vulnerabilities were identified. Input validation, sanitization, and server-side defenses effectively prevented malicious payloads. While an area for hardening was noted, no issues were found that compromise the security of the application.

Remediation Testing Summary

Echelon conducted remediation testing on the medium risk finding on April 30th, 2025. After a new deployment, Echelon observed the endpoint properly rate limits requests and a brute-force attack is heavily restricted and limited to just a few requests before restricting access. The medium-risk issue has been successfully remediated.

Dashboard

OBSERVATION COUNT

Critical Risk Observations	0
High Risk Observations	0
Medium Risk Observations	0
Low-Risk Observations	0

TIMELINE

04/21/2025	Testing Start Date
04/28/2025	Testing End Date
04/28/2025	Draft Report Delivery
04/30/2025	Remediation Testing

SECURITY OBSERVATIONS LIST

ID	TITLE	RISK	ROOT CAUSE
APP-01	Insufficient Brute Force Protection	REMEDIATED	*Insecure Configuration*

SCOPE

Web Application penetration testing and vulnerability scanning were performed on the following scope:

- pentest.staging.pequity.app

TESTING DETAILS

Web Application Testing Details

WEB APPLICATION SUMMARY

Pequity engaged Echelon Risk + Cyber (Echelon) to perform a web application penetration test and vulnerability scan against Pequity's staging environment. Echelon identified one medium-risk vulnerability within the application that involves the potential for account compromise with unlimited password guess attempts. The application does not rate limit authentication requests, and a threat actor could attempt unlimited password guesses on user accounts.

Additional common attack vectors were explored during the engagement, including but not limited to input validation bypasses, SQL injection, cross-site scripting (XSS), command injection, and other forms of injection attacks. Echelon conducted extensive testing across both authenticated and unauthenticated areas of the application, targeting user-input fields, URL parameters, request headers, cookies, and API endpoints.

Client-side attack vectors, such as reflected XSS and DOM-based injection points, were also assessed through manual and automated techniques. Where appropriate, payloads were crafted to simulate real-world attacker behaviors, including attempts to manipulate client-side logic or abuse insecure JavaScript functions.

Throughout these assessments, no exploitable vulnerabilities were identified. Application-side input sanitization, validation controls, and server-side defenses consistently prevented malicious payloads from executing or impacting application behavior. Echelon recommends maintaining strong input validation routines, ongoing secure development practices, and regular security assessments to ensure the application continues to withstand evolving attack techniques.

Remediation Testing Summary

Echelon conducted remediation testing on the medium risk finding on April 30th, 2025. After a new deployment, Echelon observed the authentication endpoint properly rate limits requests and a brute-force attack is heavily restricted and limited to just a few requests before restricting access. The medium-risk issue has been successfully remediated.

WEB APPLICATION SECURITY WINS

During the Web Application Assessment, the offensive security team noted 3 positive observations that limited success of the team in gaining unauthorized access within the application.

Win	Description
	Errors were generalized and non-specific.
🔒	No code injection attempts were successful.
🔒	The application appeared to be secure, and vulnerabilities identified from previous assessments were resolved and were not identified in other areas within the application.

WEB APPLICATION SECURITY OBSERVATIONS LIST

The following table is a list of observations discovered during testing. Full information on these observations can be found in the “Detailed Observations” section.

ID	TITLE	RISK	ROOT CAUSE
APP-01	Insufficient Brute Force Protection	MEDIUM	*Insecure Configuration*

DETAILED REPORT

This section covers in detail the observations with corresponding recommendations, risk ratings, impacts, root causes, OWASP Category and details leading to the discovery of the observation.

APP–01 – Insufficient Brute Force Protection

DREAD SCORE	AFFECTED ENDPOINTS	OWASP CATEGORY	SEVERITY
15	*/api/token/both*	*Insecure Configuration*	Successfully Remediated

RECOMMENDATION

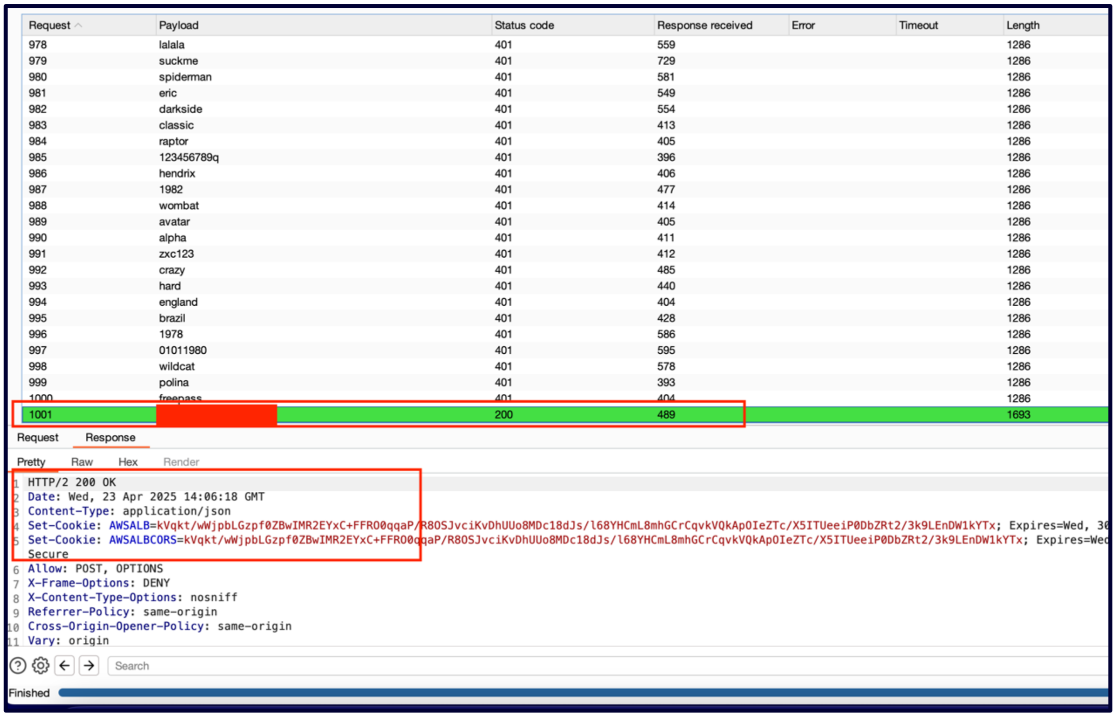
- ***Implement an Account Lockout:*** *Accounts within the application should prevent brute-force attacks by enabling rating limiting.*

IMPACT

A Threat Actor could perform unlimited brute-force attempts against the target account within the environment.

DETAILS

Echelon performed a brute-force attack against a testing account and performed 1000 known incorrect passwords, and a final successful attempt. The system did not rate limit the attempts and unlimited password guesses are accepted.



Request	Payload	Status code	Response received	Error	Timeout	Length
978	lalala	401	559			1286
979	suckme	401	729			1286
980	spiderman	401	581			1286
981	eric	401	549			1286
982	darkside	401	554			1286
983	classic	401	413			1286
984	raptor	401	405			1286
985	123456789q	401	396			1286
986	hendrix	401	406			1286
987	1982	401	477			1286
988	wombat	401	414			1286
989	avatar	401	405			1286
990	alpha	401	411			1286
991	zxc123	401	412			1286
992	crazy	401	485			1286
993	hard	401	440			1286
994	england	401	404			1286
995	brazil	401	428			1286
996	1978	401	586			1286
997	01011980	401	595			1286
998	wildcat	401	578			1286
999	polina	401	393			1286
1000	freepass	401	404			1286
1001	[redacted]	200	489			1693

```
HTTP/2 200 OK
Date: Wed, 23 Apr 2025 14:06:18 GMT
Content-Type: application/json
Set-Cookie: AWSALB=kVqkt/wWjpbLGzpf0ZBwIMR2EYxC+FFRO0qqaP/R8OSJvciKvDhUUo8MDc18dJs/l68YHCmL8mhGCrCqvkVQkApOIeZTc/X5ITUeeiP0DbZRt2/3k9LEnDW1kYTx; Expires=Wed, 30
Set-Cookie: AWSALBCORS=kVqkt/wWjpbLGzpf0ZBwIMR2EYxC+FFRO0qqaP/R8OSJvciKvDhUUo8MDc18dJs/l68YHCmL8mhGCrCqvkVQkApOIeZTc/X5ITUeeiP0DbZRt2/3k9LEnDW1kYTx; Expires=Wed
Secure
Allow: POST, OPTIONS
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Vary: origin
```

WEB VULNERABILITY SCANNER – SUMMARY

Title	Risk	Host

No significant issues were identified.

Summary of Results

Echelon conducted an external network vulnerability assessment targeting the application’s supporting infrastructure. A comprehensive external scan was performed using industry-standard vulnerability scanning tools to identify potential risks such as open ports, outdated services, misconfigurations, and known vulnerabilities.

The assessment found no significant vulnerabilities affecting the external network or infrastructure components. SSL/TLS certificates were properly deployed, with strong cipher suites and appropriate configurations to ensure secure communications. Additionally, the automated scanning results indicated that no exploitable vulnerabilities were present within the externally exposed services.

While no significant findings were observed, Echelon recommends continued monitoring, routine patch management, and periodic external vulnerability scans to maintain a strong security posture over time.

APPENDIX A – DREAD SCORING

The following table summarizes the calculation of DREAD Scoring:

Damage Criteria	Critical (Score: 10)	High (Score: 7)	Medium (Score: 4)	Low (Score: 1)
Damage Potential	A threat actor can gain full access to the system; execute commands as root/administrator	A threat actor can gain non-privileged user access, leaking extremely sensitive information	Sensitive information leak; Denial of Service	Leaking trivial information
Reproducibility	The attack can be reproduced every time and does not require a timing window	The attack can be reproduced most of the time	The attack can be reproduced, but only with a timing window	The attack is very difficult to reproduce, even with knowledge of the security hole
Exploitability	No programming skills are needed; automated exploit tools exist	A novice threat actor could execute the attack in a short time	A skilled threat actor could create the attack, and a novice could repeat the steps	The attack required a skilled threat actor and in-depth knowledge every time to exploit
Affected Users	All users, default configuration, key customers	Most users; common configuration	Some users; nonstandard configuration	Very small percentage of users; obscure features; affects anonymous users
Discoverability	Vulnerability can be found using automated scanning tools	Published information explains the attack. The vulnerability is found in the most commonly used feature	The vulnerability is in a seldom-used part of the product, and few users would come across it	The vulnerability is obscure, and it is unlikely that it would be discovered

Risk Rating	DREAD Score	Risk Description
Critical	40-50	**Critical observations pose an extreme risk to your system/network/application, with the potential for exploitation by even non-authenticated or external threat actors. The exploitation of such observations could lead to a threat actor gaining privileged access, root or admin rights, potentially causing severe disruptions to your business operations and continuity. We recommend that the remediation process for these operations begin immediately upon discovery.**
High	25-39	**A high observation poses a significant threat to your system/network/application/control. The potential exploitation of the observation could result in non-privileged access to a system, escalation of privileges, or even considerable information disclosure. Following the remediation of critical risks, high-risk observations should be prioritized in a short action 10-day plan.**
Medium	11-24	**A Medium observation poses a notable risk to your system/network/application/control. The exploitation of these observations could lead to sensitive data exposure or access to a system/network/application/control with a non-privileged user. While these do not pose a substantial threat to business operations, their remediation is still important. We recommend adding these observations to a 60-day remediation plan, ensuring they are addressed only after higher priority risks have been mitigated.**
Low	1-10	**A low observation poses a minor risk to your system/network/application/control and is often exceedingly difficult to exploit or results in minimal risk to the business. However, over time, even low-risk observations can become problematic if left unaddressed. We recommend incorporating these vulnerabilities into a 3-month remediation plan, allowing your system/network/application/control to maintain optimal security health long term**

APPENDIX D – OWASP CATEGORY DESCRIPTIONS

The following table summarizes the OWASP categories and descriptions:

OWASP Category	Description
Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data
Cryptographic Failure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
Insecure Design	Insecure design is a broad category representing different weaknesses, expressed as "missing or ineffective control design. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.
Security Misconfiguration	Commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information.
Vulnerable and Outdated Components	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
Identification and Authentication Failures	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
Software and Data Integrity Failures	Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application.
Security Logging & Monitoring Failures	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data.
Server-Side Request Forgery	SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).