March 26, 2025

To,

Aeologic Technologies
Pinnacle Tower, 1st Floor 101,
A – 42/6, Sector 62 - 201301

Dear Sir,

Sub: Proposal for Conducting Security Audit of NCSC Web Application.

We thank you for the opportunity given to us for applying to undertake website Security Audit of http://ncscuat.aeologic.in/

We hope you find everything in order. Thanking you and hoping to hear from you soon. If you need any further information / clarification, please feel free to contact the undersigned.

Regards,

For AAA Technologies Limited

Anjay Agarwal
Chairman & Managing Director
B.Com, LL.B(Gen), F.C.A., Grad. CWA, A.C.S., C.I.A. (USA), C.F.E. (USA), C.I.S.A. (USA), PGDFERM, I.S.A., D.I.R.M., BS7799 Certified Lead Implementer, A.B.C.I.(U.K.), ISO 27001 Certified Lead Implementer, ISO 27001 Certified Lead Auditor, BCMS Certified Lead Implementer, CGEIT (USA), CEH, ECSA& LPT COBIT Certified Assessor, CISA Certificate No.: 23850

Table of Contents

Web Application Scope of Work

Sr. no	Attack Type	Description
1.	**A1- 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.
2.	**A2- Broken Authentication**	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.
3.	**A3-Sensitive Data Exposure**	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. 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.
4.	**A4-XML External Entities (XXE)**	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks
5.	**A5-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, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc

6.	**A6-Security Misconfiguration**	Security misconfiguration is the most commonly seen issue. This is 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. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
7.	**A7-Cross-Site Scripting (XSS)**	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
8.	**A8-Insecure Deserialization**	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
9.	**A9-Using Components with Known Vulnerabilities**	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
10.	**A10 Insufficient_Logging &Monitoring**	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. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Procedure for conduct of Website Security Audit

a) After receiving the work order and details as mentioned above, we would be conducting first round of security audit.

b) If we find any vulnerability we will communicate the same to you and you will ensure and remove the vulnerabilities.

c) You will then communicate to us that the vulnerabilities have been removed. Thereafter, we shall conduct the final round of audit & send you the report.

d) In case, any subsequent or more audit is required to be conducted then that would be charged extra as stated in the professional fees

e) We will take 9 -to 10 working days to start the audit.

f) The audit does not include risk mitigation.

g) The security audit would be conducted offsite.