Website Security Audit Report

DOE portal for information dissemination and DOE API Service

October 2023

AAA Technologies Ltd
278-280, F Wing, Solaris-1,
Saki Vihar Road, Opp. L & T Gate No. 6,
Powai, Andheri (East),
Mumbai 400 072, INDIA
Tel: + 91 22 28573815 / 16
Fax: + 91 22 40152501
info@aaatechnologies.co.in
www.aaatechnologies.co.in

Accurate. Reliable. Innovative.

Table of Contents

Document Reference

Item	Description
Document Title	Website Security Audit Report
Department	IT Department
Version No.	1.0
Status	Final
File Name	DOE portal for information dissemination and DOE API Service - Website Security Audit Report-Final
Type	Word Document
Owner	IT Department

Control Page

Document Amendment Record			
Change No.	**Date**	**Prepared by**	**Brief Explanation**
1.0	17/10/2023	AAA Technologies Ltd	Final Report

1 Executive Summary

1.1 Introduction

AAA Technologies Limited ('AAA') was engaged by National Informatics Centre Services Inc. (NICSI) to perform website security audit of DOE portal for information dissemination and DOE API Service. The report highlights gaps identified and recommendations to remediate the gaps.

1.2 Objectives of Audit

The objectives of audit were to provide independent evaluation of the status of controls of DOE portal for information dissemination and DOE API Service Website. The main purpose of the test is to determine any security vulnerabilities in the website as specified in the scope. The tests are carried out assuming the identity of an attacker or a user with malicious intent

1.3 Scope of Audit

The scope of work was to carry out Penetration Testing of the website of DOE portal for information dissemination and DOE API Service by making attempts to uncover known vulnerabilities viz.
(http://doe.wbpower.gov.in/audit) as per Open Web Application Security Project (OWASP) top ten criteria

1.4 Approach

During the course of this review we assessed the vulnerabilities in accordance with OWASP Top 10 Vulnerabilities and also for other known web application vulnerabilities. Our tests into divided into two parts namely Automated checks and Manual checks

1.5 Disclaimers and Restrictions

- Organisation's management is responsible for its assertions. Our responsibility is to express an opinion on management's assertion based on our audit.
- The audit was conducted in accordance with the Information Systems Auditing Standards issued by the Standards Board of Information Systems Audit and Control Association. Further, the objective of the audit was to obtain reasonable assurance that the assertion is not materially misstated. Our audit included (1) Obtaining an understanding of the objectives; (2) selectively testing these objectives; (3) testing and evaluating; and (4) performing such other procedures as we considered necessary under the circumstances. We believe that our audit provides a reasonable basis for our opinion.
- Because of inherent limitations in controls, errors or fraud may occur and may not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.
- This report is strictly to be used for the intend purpose of compiling the controls being followed for the purposes of analysis and improvement.
- It is firmly recommended to test out all our technical recommendations to the system internals such as services or registry in a test environment and the impact on the reliability and integrity of the system be evaluated before rolling out the changes to the production environment.
- This report does not include any representation on the financial, marketing, human resources or any other health of the Organisation or on the future viability of the Organisation or minimizing or exposure of all risks associated with computerized environment, due to its inherent limitations.

1.6 Summary of Significant Findings and Recommendations

1) Our detailed observations and recommendations are attached herewith.

2) Below listed table indicates summary of Penetration Testing attacks conducted by us. We have used following legends for the attached sheet
   a. Not Successful - This means that the Test conducted but the website is not vulnerable to this attack.
   b. Successful – This means that the Test conducted and the website is found to be vulnerable or may be vulnerable to this attack

Sr. no	Attack Type	Description	Penetration Testing status
1.	A1- Injection	Injection flaws, such as SQL, 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 unauthorized data	Not Successful
2.	A2- Broken Authentication	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities	Not Successful

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.	Not Successful
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.	Not Successful
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.	Not Successful

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.	Not Successful
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.	Not Successful
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.	Not Successful

9.	A9-Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.	Not Successful
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.	Not Successful

1.7 Conclusion

In our opinion and based on our examination and explanations given to us, our Penetration Testing does not reflect vulnerability subject to as stated in the certificate, if any in the website of DOE portal for information dissemination and DOE API Service and the website may be allowed to be hosted.

For AAA Technologies Limited

ANJAY RATANLAL AGARWAL

Digitally signed by ANJAY RATANLAL AGARWAL
DN: c=IN, o=AAA TECHNOLOGIES LIMITED, 2.5.4.20=263c3649bd396c5ce504937e9cda03a0a25e9310ca648b884e2f1d697947a4c3, ou=DIRECTOR,CID - 6902346, postalCode=400072, st=Maharashtra, serialNumber=f22174cfcef7a586f7c4b0793eee29b4ed4b4f265b311c2c9ba8a1898fbb46a3, cn=ANJAY RATANLAL AGARWAL
Date: 2023.10.17 17:23:01 +05'30'

Anjay Agarwal
Chairman and Managing Director
B.Com, LL.B(Gen), F.C.A., A.C.M.A., 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), CRISC (USA), CEH, ECSA, LPT

Place: Mumbai
Dated: October 17, 2023

2 Detailed Website Security Report

2.1 A1- Injection

1) A1- Injection	
Abstract	Injection flaws, such as SQL, 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 unauthorized data
Ease of Exploitation	Easy
Impact	Injection can result in data loss or corruption, lack of accountability, or denial of access. Injection can sometimes lead to complete host takeover
Observation	No significant vulnerability that can be potentially used by an attacker
Recommendations	None
Snapshot	None

2.2 A2- Broken Authentication

2) A2- Broken Authentication	
Abstract	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities
Ease of Exploitation	Average
Impact	Such flaws may allow some or even all accounts to be attacked. Once successful, the attacker can do anything the victim could do. Privileged accounts are frequently targeted
Observation	No significant vulnerability that can be potentially used by an attacker
Recommendations	None
Snapshot	None

2.3 A3- Sensitive Data Exposure

3) A3- Sensitive Data Exposure	
Abstract	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
Ease of Exploitation	Easy
Impact	Attackers typically don't break crypto directly. They break something else, such as steal keys, do man-in-the-middle attacks, or steal clear text data off the server, while in transit, or from the user's browser.
Observation	No significant vulnerability that can be potentially used by an attacker
Recommendations	None
Snapshot	None

2.4 A4- XML External Entities (XXE)

4) A4- XML External Entities (XXE)	
Abstract	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.
Ease of Exploitation	Difficult
Impact	Attackers can exploit vulnerable XML processors if they can upload XML or include hostile content in an XML document, exploiting vulnerable code, dependencies or integrations.
Observation	No significant vulnerability that can be potentially used by an attacker
Recommendations	None
Snapshot	None

2.5 A5- Broken Access Control

5) A5- Broken Access Control	
Abstract	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.
Ease of Exploitation	Difficult
Impact	The technical impact is attackers acting as users or administrators, or users using privileged functions, or creating, accessing, updating or deleting every record. The business impact depends on the protection needs of the application and data.
Observation	No significant vulnerability that can be potentially used by an attacker
Recommendations	None
Snapshot	None

2.6 A6- Security Misconfiguration

6) A6- Security Misconfiguration	
Abstract	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
Ease of Exploitation	Average
Impact	Attackers can cause victims to change any data the victim is allowed to change or perform any function the victim is authorized to use
Observation	No significant vulnerability that can be potentially used by an attacker
Recommendations	None
Snapshot	None

2.7 A7- Cross Site Scripting (XSS)

7) A7- Cross-Site Scripting (XSS)	
Abstract	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. 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
Ease of Exploitation	Average
Impact	Attackers can execute scripts in a victim's browser to hijack user sessions, deface web sites, insert hostile content, redirect users, hijack the user's browser using malware, etc.
Observation	No significant vulnerability that can be potentially used by an attacker
Recommendations	None
Snapshot	None

2.8 A8- Insecure Deserialization

8) A8- Insecure Deserialization	
Abstract	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.
Ease of Exploitation	Difficult
Impact	The impact of deserialization flaws cannot be overstated. These flaws can lead to remote code execution attacks, one of the most serious attacks possible. The business impact depends on the protection needs of the application and data.
Observation	No significant vulnerability that can be potentially used by an attacker
Recommendations	None
Snapshot	None

2.9 A9- Using Components with Known Vulnerabilities

9) A9- Using Components with Known Vulnerabilities	
Abstract	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
Ease of Exploitation	Average
Impact	Attacker identifies a weak component through scanning or manual analysis. He customizes the exploit as needed and executes the attack. It gets more difficult if the used component is deep in the application.
Observation	No significant vulnerability that can be potentially used by an attacker
Recommendations	None
Snapshot	None

2.10 A10- Insufficient Logging & Monitoring

10) A10- Insufficient Logging & Monitoring	
Abstract	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.
Ease of Exploitation	Easy
Impact	Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident. Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected.
Observation	No significant vulnerability that can be potentially used by an attacker
Recommendations	None
Snapshot	None