This is a sample report created by the Azacus.io team and does not contain information from any client nor should be taken as an exact sample of a final report.

AZACUS.IO

CYBERSECURITY

FINAL REPORT #T9123

Web Application Penetration Test

Egara Trading Ltd.

July 2019

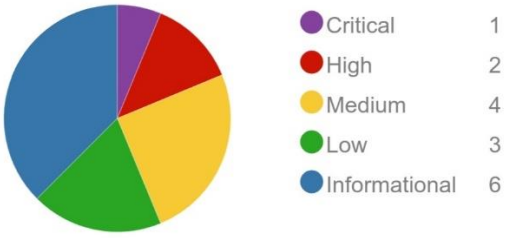
Table of Contents

OVERVIEW

SYNOPSIS

Azacus.io were engaged to evaluate the security of Egara Trading's (Ltd.) AAXD Web Application during the course of a two-week period in July 2019. The goal of the assessment was to identify security vulnerabilities in ETL's internet facing systems and services. All issues identified by Azacus have been manually verified and exploited, where applicable, to demonstrate the underlying risk to ETL, its employees and clients.

KEY FINDINGS



During this assessment, multiple vulnerabilities were uncovered, amongst which one (1) was critical, two (2) were high, four (4) were rated medium risk and three (3) and six (6) as low and informational respectively. While none of the recorded vulnerabilities presented a direct high risk from an external attacker to fully compromise the Integrity or Availability of the data or its underlying infrastructure, it was noted that several systems could be targeted from an unauthenticated user with a low to medium impact on the Confidentiality of the client's infrastructure.

- REFLECTED XSS – The application did not adequately sanitize user supplied input. It was possible to inject reflected JavaScript code into several application pages and thereby target its users. An attacker could use this vulnerability to perform attacks against the users' web browsers and deface application pages by adding malicious scripts to the application.

- EXCESSIVE PORTS EXPOSED – Several network ports were found to be exposed during the infrastructure assessment, multiple of them being critical services such as SSH or Databases. Although there were security measures in place it is industry good practices to not expose them to the wide web.

- SENSITIVE FILES DISCLOSURE – It was noted that two instances of an Apache web service exposed several web logs to an unauthenticated user. While the accessible logs date from 2016 it could allow an attacker to extract internal information from a 3rd party server, internal software used, full path disclosure, token URLs, etc.

STRATEGIC RECOMMENDATIONS

Azacus.io recommend considering the implementation of the following:

- IMPLEMENT TWO-FACTOR AUTHENTICATION ON PUBLIC FACING SYSTEMS. Internet facing systems are regularly being probed and attacked. Extra care needs to be

taken on these systems to prevent unauthorized access.

- STRENGTHEN PASSWORD REQUIREMENTS. ETL should use technical means to ban known bad/weak passwords and train users on safe password practices.
- REQUIRE DEFENSIVE CODING TRAINING FOR DEVELOPERS. Developers are the first line of defense when it comes to custom web applications. Developers should be made aware of the common mistakes that lead to vulnerabilities and learn ways to prevent these issues before the code is run on production systems.

EXECUTIVE SUMMARY

[This section will contain a high level non-technical summary of the most important findings during the engagement. The aim of the Executive Summary is to translate technical jargon to more accessible and understandable language for decision makers, compliance officers and other non-technical stakeholders.]

.

VULNERABILITIES SUMMARY

TABLE OF FINDINGS

	ID	Title	Category	Rating
	T9123-AAXD-001	Broken Access Control	Access Control	Critical
	T9123-AAXD-003	Example	Authentication	High
	T9123-AAXD-008	Verbose HTTP Headers	Information Disclosure	Low
	T9123-AAXD-009	Example	Input Validation	Low
	T9123-AAXD-0011	Example	Authentication	Informational
	T9123-AAXD-0016	Example	Outdated Software	Informational

CLASSIFICATION OF VULNERABILITIES

The rating system assesses the risk associated with a vulnerability in terms of attack likelihood and potential impact.

- Impact is derived from: loss of integrity, confidentiality and availability.
- Likelihood is derived from: existence of a publicly known successful exploit, the level of access required and the ease of exploitation.

Each vulnerability or identified risk has been labeled as a vulnerability and categorized as a Critical Risk, High Risk, Medium Risk, Low Risk or as Informational.

 Critical Risk	Should be addressed promptly. Immediate danger to the target's infrastructure/application. May allow an attacker gain unauthorised access to the system.
 High Risk	Should be addressed promptly. Significant danger to the target's infrastructure/application. May allow an attacker to escalate privileges, access confidential data or execute a denial of service. These findings could also be combined to reach a Critical Risk rating.
 Medium Risk	Should be addressed in a timely manner. Successful exploitation requires time, effort and multi-skilled knowledge Successful exploitation may require client's interaction These findings could also be combined to reach a High or Critical Risk rating.
 Low Risk	Should be registered and can be addressed at a later time. May not pose a direct security risk but may introduce suboptimal configuration or result in information disclosure.
 Informational	No adverse impact identified during the assessment. These issues are for informational purposes.

The weighting of these values is dependent upon the specified risk priorities and the consultant's understanding of the scope.

TECHNICAL DETAILS

OBJECTIVE

The primary objective of the assessment was to **understand** the weaknesses intrinsic of the application's context and **asses** the effectiveness of the security measures as well as good industry practices that prevent attackers compromising the information stored and processed by the application or its underlying infrastructure.

SCOPE

The scope of the testing performed was restricted to the applications below:

- https://azacus.io
- https://beta.azacus.io

TEST LIMITATIONS

[Example: testing was delayed until 12pm on the first day as permission from HOSTING DOT COM had not been granted.]

TECHNICAL SUMMARY

If applicable

GOOD PRACTICES

[This section will summarise the client's industry good practices enforced within the scope according to cybersecurity standards, controls, procedures and recommendations such as OWASP Top 10, OSSTMM 3 and/or SANS T20.]

CRITICAL RISK ISSUES

T9123-AAXD-001 – BROKEN ACCESS CONTROL

Critical Risk

Summary

By altering the intended workflow of the application, it was possible to bypass its original sequence allowing unauthenticated users to perform actions outside the approved business logic and accessing restricted documents.

Description

Web applications functionalities verify function level access rights before making that feature available to the User Interface (UI). However, applications need to perform the same access control checks on the server when each function is accessed every time. Relying on presentation layer access controls (e.g. hiding links) provides insufficient protection against unauthorised access. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

Impact

It was possible for the consultant to break the business logic of the application and bypass the "delete functionality", which consequently made the report file available on the server indefinitely. It is important to mention that, as a result, the file report could be accessed, by default, from an unauthenticated user.

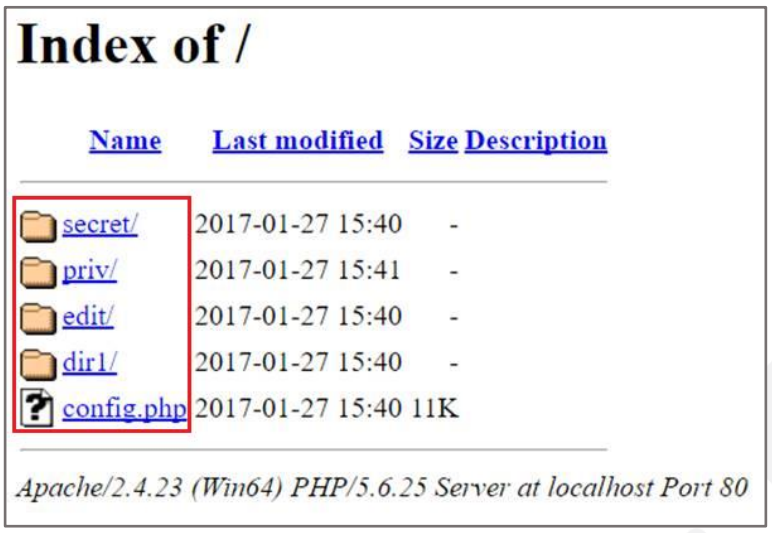


Figure 1 - Screen Capture showcasing the consultant accessing restricted documents

Affected Systems

- https://beta.azacus.io

Recommendations

Azacus.io recommend implementing consistent and easy to analyse authorisation module that is invoked from all the business functions. Frequently, such protection can be provided by one or more components external to the application code. Consider the process for managing entitlements and ensure they can be updated and audited easily. Never hard-code authorisation controls.

The enforcement mechanism(s) should deny all access by default, requiring explicit grants to specific roles for access to every function. If the function is involved in a workflow, check to make sure the conditions are in the proper state to allow access. Do not rely on not displaying links and buttons to unauthorised functions with the User Interface, as this "presentation layer access control" does not actually provide protection. Implement additional checks in the controller or business logic.

References

https://cwe.mitre.org/data/definitions/306.html

https://www.owasp.org/index.php/Top_10-2017_A5-Broken_Access_Control

HIGH RISK ISSUES

T9123-AAXD-008 – VERBOSE HTTP HEADERS

Low Risk

Summary

Lorem ipsum dolor sit amet, nascetur lorem, commodo suspendisse ac commodo, tellus mi hac. Sit enim, quam dolorem mauris in vitae quam, rhoncus nulla tellus at nullam, neque aut. Non elementum sit erat odio vel..

Description

Sed at turpis mus lorem nibh, et quis, in urna congue nulla sed. Blandit bibendum euismod integer ultricies montes lobortis. Aenean aliquam aliquam, enim aliquet ante, eu pede leo sodales sed condimentum nulla, nam ut natoque nullam ut habitasse ut facilisi odio orci, faucibus eget suspendisse dolor ullamcorper, nulla quis. Ridiculus.

Impact

Aenean aliquam aliquam, enim aliquet ante, eu pede leo sodales sed condimentum nulla, nam ut natoque nullam ut, nibh posuere. Enim magnis mauris dis wisi pede viverra.

HTTP Request

```
GET /u/login/ HTTP/1.1
Host: pentest.ClientsName.com
```

HTTP Response:

```
HTTP/1.1 200 OK
[...]

Content-Length: 16168

Connection: close
Server: nginx/1.10.3 (Ubuntu)
Expires: -------
Vary: Cookie, Accept-Encoding
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Set-Cookie: csrftoken=AAjTOTN [...] donzt1QexW
```

Affected Systems

- https://beta.azacus.io

Recommendations

Sed at turpis mus lorem nibh, et quis, in urna congue nulla sed. Blandit bibendum euismod integer ultricies montes lobortis. Aenean aliquam aliquam, enim aliquet ante, eu pede leo sodales sed condimentum nulla, nam ut natoque nullam ut, nibh posuere. Enim magnis mauris dis wisi pede viverra, vel sapien eu rutrum penatibus, nulla habitasse ut facilisi odio orci, faucibus eget suspendisse dolor ullamcorper, nulla quis..

References

https://example.html

https://www.owasp.org/

ENGAGEMENT DETAILS

DESCRIPTION

The primary objective of the assessment was to understand the weaknesses intrinsic of the application's context and asses the effectiveness of the security measures as well as good industry practices that prevent attackers compromising the information stored and processed by the application or its underlying infrastructure.

ENGAGEMENT LIMITATIONS

This engagement reviewed a snapshot in time of the systems in scope. Underlying configuration changes could result in the addition of new issues or a weakened security standpoint. New vulnerabilities and attack vectors are discovered on a daily basis encouraging the need for further security testing. Penetration testing is a security standard representative of both Azacus' security assessment methodology and attack techniques publicly known at the time of the engagement. As project's scope and time constraints do not limit real world attackers, it is possible that additional security weaknesses, which could not reasonably be identified during the engagement, may be present and exploited in the future.

CUSTOMER DETAILS

Customer:

	Name	e-Mail	Mobile number
Management Contact			
Technical Contact			
Emergency Contact			

SCOPE

The scope of the testing performed was restricted to the applications below:

- https://azacus.io
- https://beta.azacus.io

ENGAGEMENT'S DURATION

Start Date	Finish Date
15 July 2019	25 July 2019

TEAM

- John Doe Toledano (one@azacus.io)
- Jane Doe (two@azacus.io)

This is a sample report created by the Azacus.io team and does not contain information from any client nor should be taken as an exact sample of a final report.

DOCUMENT CONTROL

Date	Version	Name	Comments
25 July 2019	0.1	John Doe	Initial Draft
26 July 2019	0.2	Jane Doe	Internal QA
	0.3		Technical QA
27 July 2019	1.0		Final Report

AZACUS.IO

CYBERSECURITY