NETTITUDE
AN LRQA COMPANY

Penetration Testing Technical Report

Prepared For: AZETS
Target: AZETS WEB APPLICATIONS
Author: STAVROS MANIS
Date: 13 May 2022
Version: 2.0

Confidential Security Document

Contents

1 Document Distribution List

Nettitude	Name	Title
	Stavros Manis	Security Consultant
	Nikhil Keshwala	Security Consultant
	Sumit Siddharth	Security Consultant
	Pedro Oliveira	Security Consultant
	Ben Keighley	Account Manager

Azets	Name	Title
	Derek Hans	Head of Technology
	Shahzeb Iqbal	Active Head of Technology
	Kenneth Matson	Managing Director

2 Revision History

Version	Issue Date	Issued by	Comments
0.1	23 November 2021	Sumit Siddharth	Initial Draft
0.2	30 November 2021	Pedro Oliveira	Quality Assurance
0.3	06 December 2021	Ben Keighley	Quality Assurance
1.0	07 December 2021	Sumit Siddharth	Final version
1.1	29 April 2022	Stavros Manis	Retest Initial Draft
1.2	12 May 2022	Nikhil Keshwala	Quality Assurance
1.3	12 May 2022	Ben Keighley	Quality Assurance
2.0	13 May 2022	Stavros Manis	Retest Final Version

3 Engagement Particulars

Background

This report serves as technical documentation for the recent penetration test performed for Azets by Nettitude. For a high-level assessment of the tested environment, please refer to the associated management report:

```
MGMT_REPORT_Penetration_Test_Azets_Azets_Web_Applications_2022-04-29_v2.0.pdf
```

Rules of Engagement

The assessment was performed in line with the following rules of engagement:

- Nettitude's grey box testing methodology was used.
- Social engineering was not permitted.
- Denial of Service (DoS) testing was not permitted.
- The engagement was conducted from Nettitude's remote attack platform, which was located at 193.36.8.0/21.
- The testing and reporting were permitted and performed during a one-day period; 29 April 2022. The testing period corresponds to the timeframe given to retest the original findings enumerated during the original web application penetration test performed on 15th of November 2021. Any results held in this report relate to the status of the tested environment on those dates.

Scope

Azets tasked Nettitude to perform a security assessment with the following scope:

Component	Description
https://idp-develop-proddb.staging.cozone.com	Identity Provider Application
https://documents-develop-proddb.staging.cozone.com/ui/	File Transfer application

https://payroll-develop-proddb.staging.cozone.com/ui/	Employee Application

User Accounts

Nettitude made use of the following accounts to ensure that breadth of testing, as well as user related testing, was achieved:

Username	Application	Role
consultant@test.com	File Transfer Application	Consultant
drive@test.com	File Transfer Application	Client
employee@test.com	Employee Application	Employee
employee2@test.com	Employee Application	Employee
manager@test.com	Employee Application	Manager

Testing Windows Observations and Constraints

The time frame provisioned for the completion of this engagement was adequate. No constraints were encountered during the engagement.

Findings Summary

During the engagement, a total number of three findings were identified. The following table shows the categorisation by severity:

0	0	0	1	0
Critical	High	Medium	Low	Info.

4 Findings

4.1 Azets Web Applications Test

Component	Description	Severity	Recommendation	Ref.
https://documents-current-proddb.staging.cozone.com https://payroll-current-proddb.staging.cozone.com	No Concurrent Session Management	Low	Allow users to review and terminate any sessions under their account	5.1

5 Analysis: Azets Web Applications Test

5.1 Low: No Concurrent Session Management

5.1.1 Description of the Issue

The application allowed users to establish multiple sessions, from multiple locations or browsers. The application held sensitive information and therefore a mechanism should be provided whereby the user can review all current live sessions, with the option to revoke any at will. OWASP ASVS level 2 (V3.3.3) states:

Verify that the application gives the option to terminate all other active sessions after a successful password change (including change via password reset/recovery), and that this is effective across the application, federated login (if present), and any relying parties.

An attacker in possession of compromised credentials, would be required to perform no evasion techniques such as log spoofing or log erasure as all actions carried out by the attacker would be indistinguishable from the valid user's actions, due to the concurrent session.

In addition, failure to prevent concurrent logins may permit a potentially compromised account to go unnoticed by the legitimate user as 'illegitimate' and 'legitimate' usage could occur in unison without one affecting the other. The ability to logon at multiple locations can also result in concurrency issues, if a data set updated simultaneously or from alternative sessions.

Nettitude identified that the application “documents-current-proddb.staging.cozone.com” allowed to access the user account in two different browsers at the same time due to lack concurrent session validation, as shown in the below figure:

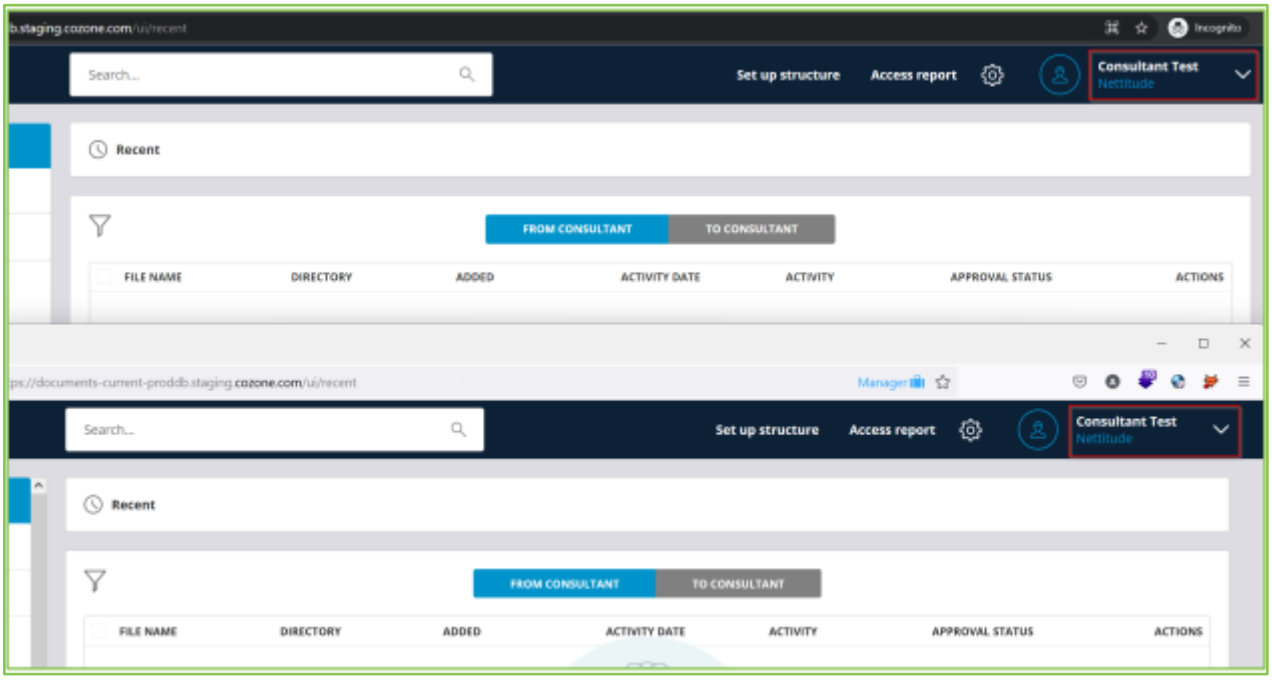

Figure 1: Concurrent sessions are allowed.

5.1.2 Affected Components

- https://documents-current-proddb.staging.cozone.com
- https://payroll-current-proddb.staging.cozone.com

5.1.3 Nettitude Recommends

1 Assess the application and its functionality and if required prohibit concurrent sessions;

2 Place further checks within the application to terminate any previous sessions, should the user log in from another location, informing the user of the reason they were logged out (this can alert a user to the fact their account is being accessed elsewhere);

3 Record the concurrent login within the application logs, to aid investigative or fraud purposes;

4 Allow the application to inform the user of their last logon date and time.

5.1.4 Further Reading

- OWASP - https://www.owasp.org/index.php/Session_Management_Cheat_Sheet

6 Appendix

6.1 Severity Rating Matrix

The severity rating is determined by the likelihood and impact of a vulnerability on a system and, where possible, in the context in which that vulnerability is exposed, e.g. remote attack vs. internal attack. The table below is used to calculate the overall severity rating of an issue based on these criteria.

This is not an assessment of risk as it does not include a valuation of the data or system, but it does provide the ability to prioritise the vulnerabilities identified within the target system or application and to integrate into their own risk management systems.

Impact

	Negligible	Minimal	Moderate	Major	Catastrophic
Rare	LOW	LOW	LOW	MEDIUM	HIGH
Unlikely	LOW	LOW	MEDIUM	HIGH	CRITICAL
Moderate	LOW	MEDIUM	MEDIUM	HIGH	CRITICAL
Likely	MEDIUM	MEDIUM	HIGH	CRITICAL	CRITICAL
Very Likely	MEDIUM	HIGH	HIGH	CRITICAL	CRITICAL

6.1.1 Likelihood

The likelihood rating of a vulnerability encompasses both the likelihood of the vulnerability being identified and attacked as well as the likelihood of that attack being successful. This is evaluated by taking into consideration the following elements:

Exploitability

- Difficulty and technical knowledge or skill required to identify/exploit the issue
- Time or resources required to mount a successful attack
- Availability of exploit code and automated attack tools

Reproducibility

- Ease of reproducing a successful attack
- Additional requirements for the attack to be successful, for example:
    - Victim user must be logged in
    - Some level of interaction by the victim user is required

Discoverability

- Number of instances of the vulnerability identified in the system
- Level of authentication required to access affected components
- Accessibility of the system (internet-facing or internal)
- Degree of specific Insider knowledge required

Frequency

- How often the issue is likely to occur over a period of time
- History of the issue in the industry
- Existence of self-propagating malware targeting the issue

These factors will be employed to formulate a final likelihood rating for a given issue.

6.1.2 Impact

The impact rating assesses the significance of exposure to a particular vulnerability. This is evaluated by considering the impacts to the affected system and the underlying business. The factors under consideration are outlined in the following table.

Impact	Negligible	Minimal	Moderate	Major	Catastrophic
Confidentiality	Disclosure of public information	Minor disclosure of commercial-in-confidence information	Major disclosure of commercial-in-confidence information	Minor disclosure of highly-confidential information	Major disclosure of highly confidential information
Integrity	Unauthorised modification of public data	Small-scale unauthorised modification of private data	Large-scale unauthorised modification of private data	Small-scale unauthorised modification of trusted data	Large-scale unauthorised modification of trusted data
Availability	Minor increase in processing load	Minor outage in a business system	Outage or unavailability of a business system	Extended unavailability or outage of a business system	Unavailability or outage of a business-critical system
Brand or Reputation	Complaints from small number of customers	Complaints from small number of customers across a broader customer base	Complaints from a large number of customers and localised media coverage	Short term adverse large scale media coverage	Extended adverse large scale media coverage
Regulatory and Legal	Warnings for minor breaches	Formal caution for regulatory breaches or threat of legal proceedings	Targeted audit / investigation by regulator or minor legal proceedings brought against the organisation	Fines imposed and negative media coverage or major legal proceedings brought against the organisation	Service line closed down

6.2 Penetration Testing Methodology

Nettitude has a series of approaches for conducting Penetration Tests.

6.2.1 Black Box Testing

In a Black Box test, the client does not provide Nettitude with any information about their infrastructure. For internal tests the customer may provide no more than a network point for the tester to connect in to. For external tests, this may simply be a URL or even just the company name that is in scope for assessment.

Nettitude is tasked with testing the environment as if they were an attacker with no information about the infrastructure or application logic that they are testing. Black Box tests tend to take longer to commission than White Box tests and may identify less exposures and vulnerabilities than those of White Box tests.

6.2.2 White Box Testing

In a White Box test, clients provide Nettitude with information about the applications and infrastructure prior to the commencement of the testing engagement. Usernames and Passwords are provided to Nettitude's testing team as part of the engagement, and the client may provide Nettitude's consultants with access to source code. In this type of testing engagement, Nettitude works closely with the client to perform the assessment. These types of tests tend to gain deeper understanding of the application and infrastructure logic, and may generate highly comprehensive test results.

6.2.3 Grey Box Testing

A Grey Box test is a blend of Black Box testing techniques and White Box testing techniques. In Grey Box testing, clients provide Nettitude with snippets of information to help with the testing procedures. This results in a highly focused test.

7 Original Findings

7.1 Azets Web Applications Test

Component	Description	Severity	Recommendation	Ref.
https://documents-current-proddb.staging.cozone.com https://idp-develop-proddb.staging.cozone.com/ https://payroll-current-proddb.staging.cozone.com https://payroll-current-proddb.staging.cozone.com/oldui/scripts/libs.all.bundle.851ca944.js	Missing HTTP Security Headers	Low	Implement the suggested HTTP headers.	Remediated
https://documents-current-proddb.staging.cozone.com https://idp-develop-proddb.staging.cozone.com/ https://payroll-current-proddb.staging.cozone.com	Outdated Client-Side JavaScript Libraries in Use	Low	Update the libraries to the latest version.	Remediated
https://documents-current-proddb.staging.cozone.com https://payroll-current-proddb.staging.cozone.com	No Concurrent Session Management	Low	Allow users to review and terminate any sessions under their account.	Not Remediated

Nettitude Penetration Testing Services

https://www.nettitude.com/penetration-testing/

NETTITUDE
AN LRQA COMPANY

UK Head Office
Jephson Court, Tancred Close, Leamington Spa, CV31 3RZ

Americas
50 Broad Street, Suite 403, New York, NY 10004

Asia Pacific
1 Fusionopolis Place, #09-01, Singapore, 138522

Europe
Leof. Siggrou 348 Kallithea, Athens, 176 74
+30 210 300 4935

Follow Us

solutions@nettitude.com
www.nettitude.com