NETTITUDE
AN LRQA COMPANY

Penetration Testing Management Report

Prepared For: WORLD DELETE
Target: World Delete App
Author: Sam Bohnel
Date: 10 February 2023
Version: 1.0

Confidential Security Document

Report Contents

The contents of this report belong to World Delete. The findings, information and recommendations in this document are for information purposes only and are based on a point in time assessment of the environment within scope. Nettitude, and the rep ort's authors, accept no responsibility for any errors, omissions, or misleading statements, in this report, or for any loss that may arise for reliance on any information and opinions expressed. Nettitude recommends that all advice and recommendations are reviewed, a risk assessment conducted and change control processes followed before any remediation work is conducted. Nettitude does not hold any responsibility for any work conducted as a result of the recommendations provided in this report.

1 High Level Assessment

World Delete engaged with Nettitude in January 2023 in order to assess the overall security posture of their World Delete App environment.

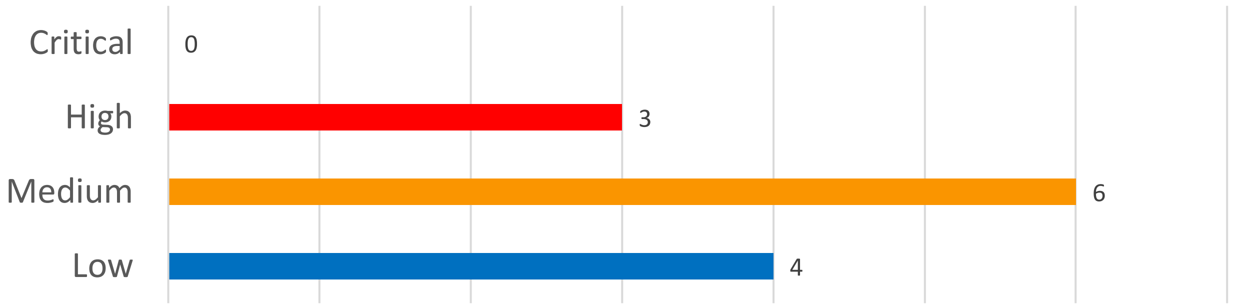
Based on World Delete’s risk profile, primary security concerns and the vulnerabilities identified at the point of the engagement, Nettitude have found the overall security posture to **require immediate attention**.

Nettitude were able to:

- Identify Access Control issues, resulting in PII disclosure.
- Upload unsafe files, that could be used to target the backend application and application users.
- Observe various authentication issues, resulting in confidentially impacts to users.

Overall Security Posture
STRONG
MODERATE
REQUIRES ATTENTION
WEAK

Vulnerabilities by Severity



Constraints and Limitations

Some limitations and constraints were encountered during the engagement, please refer to the technical report for more details.

2 Executive Summary

World Delete engaged with Nettitude in January 2023 in order to assess the overall security posture of their World Delete App environment. Testing and reporting took place over a four-day period in January 2023.

Nettiude identified several issues concerned with access controls within the application. Of note were two endpoints that revealed a large amount of personal identifiable information (PII), password hashes of the user, calendar details and photos of the user. This could be trivially exploited as the endpoints can be accessed effectively as an anonymous user, resulting in significant impact to confidentiality of the data stored in the application as well as possible financial and reputational damages. All application functionality should be sufficiently verified against the intended users access rights.

An issue with file upload functionality in application was noted, that allowed a number of malicious file types to be uploaded. The files could be used to target the backend application components as well as target users of the system. In conjunction with an access control issue identified, a determined attacker could perform phishing style attacks to target users, and harvest credentials. It is of vital importance that the file upload mechanism is reviewed, and recommendations provided in the Technical Report are applied.

A number of issues were found that weakened the overall protection of user accounts, within the application. The authentication and session management mechanism could both be improved to create a more robust configuration. The password policy in place should be improved to enforce users to create strong passwords as well as implementing account lockouts to prevent brute force style password guessing attacks. It was noted that certain accounts such as the Manger and Sales role did enforce Multi-Factor Authentication (MFA), which is good security practise.

Various other vulnerabilities are detailed in the Technical Report, that should be reviewed and the fixes should be implemented to improve the overall security posture of the application.

3 Next Steps

Nettitude recommends that World Delete perform the following post engagement activities in the order of priority indicated.

	Activity	Description	Priority
1	Debrief from Nettitude	Nettitude will deliver a formal debrief to World Delete in order to ensure that the findings of this engagement have been fully comprehended and to help assist in the formulation of a remediation plan.	++++
2	Review Access Controls	Ensure all functionality performed by the application should be verified against user permission held within the session, to prevent unauthorised access to sensitive resources, such as PII and password hashes.	+++
3	Harden the file upload mechanism	Ensure the file types allowed to be uploaded should be restricted to only those that are necessary for business functionality, to prevent dangerous files being uploaded to the application.	++
4	Harden authentication and session management	Implement the fixes detailed for the authentication and session management mechanism, to make it more robust and protect users accounts from potential compromise.	++
5	Retest	Once all the issues have been reviewed and fixes have been implemented, book a retest to ensure the fixes can be validated as fixed.	+

4 Revision History

Version	Issue Date	Issued by	Comments
0.1	31 January 2023	Sam Bohnel	Initial Draft
0.2	10 February 2023	Iain Wallace	Quality Assurance
1.0	10 February 2023	Sam Bohnel	Final version

5 Document Distribution List

Nettitude	Name	Title
	Sam Bohnel	Security Consultant
	Iain Wallace	Security Consultant

World Delete	Name	Title
	Diego Sánchez	President & Group CEO

Nettitude Penetration Testing Services

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
18 Cross Street,
#02-101, Suite S2039,
Singapore 048423

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

Follow Us

solutions@nettitude.com
www.nettitude.com