PENETRATION TESTING REPORT

CONFIDENTIAL

DOCUMENT CONTROL

CLASSIFICATION	CONFIDENTIAL	DATE	05/10/2020
VERSION NO.	2.0	DOCUMENT REFERENCE	BPEC080620-15
DOCUMENT TITLE	Bulletproof – Orlo Penetration Testing Report (retest)		
APPROVED BY	Kieran Roberts		

VERSION HISTORY

VERSION NO	DATE	AUTHOR	COMMENTS
0.1	17/07/2020	Dimitris Tsagkarakis	Document Creation
0.2	20/07/2020	Victoria Bucknell	QA
1.0	24/07/2020	Chay Donohoe	Document Approval
1.2	05/10/2020	Damian Papadamianou	Retest
2.0	12/10/2020	Kieran Roberts	Document Approval

CONTENTS

1. EXECUTIVE SUMMARY

1.1 TEST PARAMETERS

TEST REFERENCE	BPEC080620-15
TEST DATE	14/07/2020 – 16/07/2020 (Testing) 17/07/2020 (Reporting) 05/10/2020 (retest)
TEST TIME	09:00-17:00
TEST TYPE	External Web Application (Grey Box)
LIMITATIONS	No Denial of Service No Social Engineering No Load Testing
PERSONNEL	Dimitris Tsagkarakis Damian Papadamianou (retest)

1.2 RESULTS OVERVIEW

RISK LEVEL	RISKS FOUND
Critical	0
High	0
Medium	0
Low	1
Recommendations	1
TOTAL	2

AREA	DESCRIPTION	RATING
Authentication	*User authentication methods used*	STRONG
Patching	*Vulnerable software versions*	STRONG
Segmentation	*External infrastructure segmentation*	STRONG
Encryption	*Encryptions methods and protocols used*	STRONG

1.3 BUSINESS RISK SUMMARY

Bulletproof conducted a retest on the initial web application penetration test of Orlo. This was carried out from an authenticated perspective and was conducted in-line with security best practices. Overall, almost all of the previously mentioned vulnerabilities were found to be fixed however, one low-risk vulnerability still affects the application. It should also be mentioned that one medium severity vulnerability has been lowered to recommendation.

During the retest activities it was identified that the application is still vulnerable in HTML injection. Also server information is disclosed via HTTP headers response however it should be mentioned that during our email communication with the customer, we have been informed that the information disclosure issue has been fixed.

Lastly, it was found that the previously “clear text credentials” issue has been fixed and the application generates a new random password instead sending user’s password. However user can bypass the enforced change password activity without changing the generated random password.

Bulletproof recommend that Orlo resolves all issues found as a matter of urgency. Remediation advice has been provided along with the breakdown of each issue found.

1.4 TESTING METHODOLOGY

This Bulletproof penetration test used the CREST framework as an overarching methodology, into which we embedded the PTES and OWASP practices. These are specifically tailored for infrastructure and application penetration tests. Any automated tools that were used during the assessment had all plugins and signatures up to date.

1.5 SCOPE

URL	IP ADDRESS	DESCRIPTION
www.orlo.app	N/A	Static web application
app.socialsignin.co.uk	N/A	API used for www.orlo.app

Bulletproof tested the service against the following:

- Injections and input validation
- Authentication and session management
- Cross-site scripting (XSS)
- Insecure direct object references
- Security misconfiguration
- Sensitive data exposure
- Missing function-level access control
- Cross-site request forgeries
- Using components with known vulnerabilities
- Unvalidated redirects and forwards
- UI redress
- Cache control

2. PENETRATION TEST RESULTS

2.1 ENVIRONMENT OVERVIEW

The security assessment started by gathering the necessary information concerning the targets in scope to discover running services, current patch levels, improper configurations and security controls, in order to identify associated vulnerabilities and attack vectors.

2.2 CRITICALITY INDEX

Findings have been measured in-line with the CVSS scoring system as per https://www.first.org/cvss/specification-document.

RISK LEVEL	DESCRIPTION	RECOMMENDATION
CRITICAL SCORE: 9-10	A critical-risk indicates serious and immediate risk to systems and data being compromised.	Critical-rated issues need to be addressed and resolved immediately.
HIGH SCORE: 7-9	High-risk indicates that a serious weakness or exposure exists.	High-rated issues need to be addressed and resolved immediately.
MEDIUM SCORE: 4-7	Medium-risk indicates that a significant issue needs to be addressed.	Actions need to be taken once high-risks have been addressed.
LOW SCORE: 1-4	Low-risk indicates minor issues that generally are harmless but can be used when profiling an organisation.	No immediate action is required but should be addressed through the remediation phase.
RECOMMENDATIONS SCORE: N/A	Recommendations are included for improvement purposes only as they pose an indirect risk to the current environment.	N/A

2.3 RISK RESULTS

DESCRIPTION	RISK RATING	REFERENCE
~~Server-Side Request Forgery~~	~~HIGH~~	~~H-001~~
~~Session Management~~	~~MEDIUM~~	~~M-001~~
~~User Lockout~~	~~MEDIUM~~	~~M-002~~
Clear-Text Credentials	RECOMMENDATION	R-002
~~Anti-Brute Force Mechanisms Bypass~~	~~LOW~~	~~L-001~~
HTML Injection	LOW	L-002
~~Information Disclosure~~	~~RECOMMENDATION~~	~~R-001~~

2.4 WEB APPLICATION

2.4.1 SERVER-SIDE REQUEST FORGERY

~~REFERENCE~~	~~H-001~~
GOAL	Identification of Server-Side Request Forgery issues.
RESULT	During the retest activities the previously mentioned vulnerability it was found to be fixed.

DESCRIPTION

A Server-Side Request Forgery attack allows an attacker to make requests initiated by the server. As a result, an attacker is able to read and/or make changes to any accessible system from the server's network, including the server's internal network.

During the retest activities the previously mentioned SSRF vulnerability it was found to be fixed.

EVIDENCE

As it was found during the initial penetration test during the logo image upload server-side requests can also achieved using a link in the /#/settings/my-settings/my-details endpoint. The following evidence shows that the attempt was made to replicate the issue was unsuccessful. It should also be mentioned that during our email communication with the customer, customer verified that connections that were initiated during this activity were not related to customer's infrastructure.

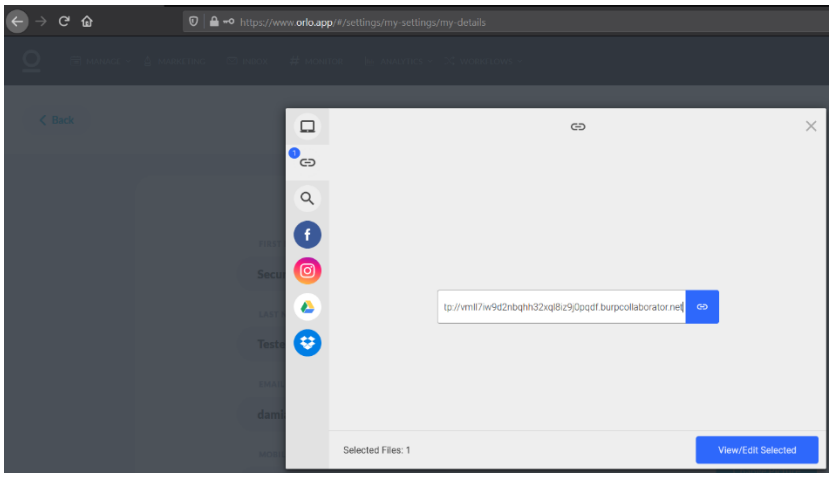

Figure 1: Logo Image Upload

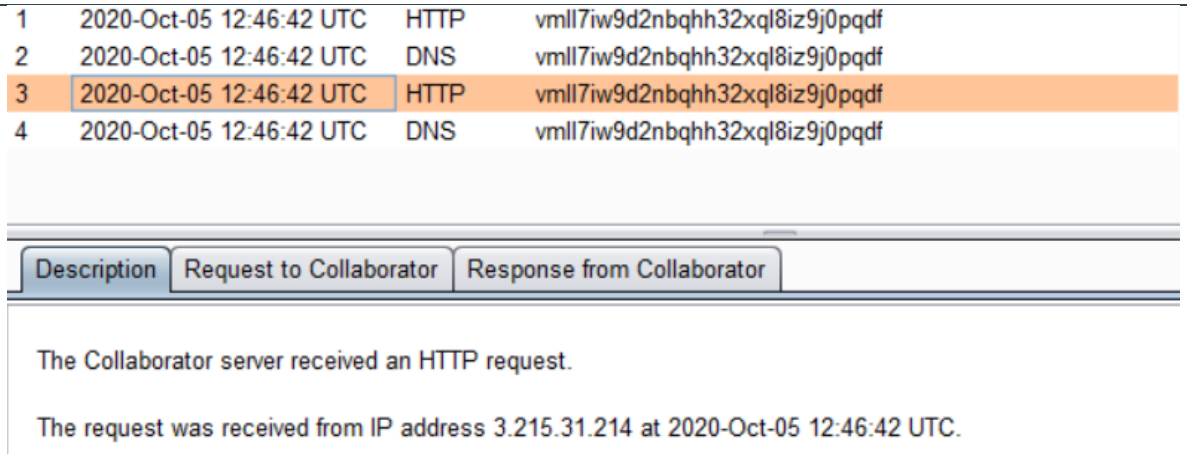

Figure 2: External Service Connections

2.4.2 SESSION MANAGEMENT

~~REFERENCE~~	~~M-001~~
GOAL	Identification of session management misconfigurations.
RESULT	During the retest activities it was found that the use of an older JWT token is not permitted.

DESCRIPTION

During the retest activities it was found that an older JWT is not valid after the generation of a new JWT.

EVIDENCE

The following request was made with an old JWT after the generation of a new JWT.

Request:

```
GET /monitoring/index HTTP/1.1
Host: app.socialsignin.co.uk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: application/json, text/plain, */*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
X-Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2MDQ0OTM3OTQsInVzZXJfaWQiOjE1OTI0LCJ0b2tlb19
pZCI6IkFYVDR5WmExcF9jRXV0NzFYRmFWIn0.ndxMadh_5WYmXyXFc0ajv_Oa_wVsgiL4QyV9652VOKo
Origin: https://www.orlo.app
Connection: close
Referer: https://www.orlo.app/
```

Response snippet (the old JWT is not valid):

```
HTTP/1.1 401 Unauthorized
Date: Mon, 05 Oct 2020 13:08:30 GMT
Content-Type: application/json
Content-Length: 84
Connection: close
Server: Apache
SSI-BackendServer: ip-172-21-11-35
Access-Control-Allow-Origin: https://www.orlo.app
Access-Control-Expose-Headers: SSI-BackendServer, SSI-TraceId
Strict-Transport-Security: max-age=36000
Cache-Control: no-cache
SSI-TraceId: X3sazn@TjhTYtdLyqT162wAAAAE

{"error":1,"message":"Request failed authentication (Invalid JWT)","error_code":401} …
```

2.4.3 USER LOCKOUT

~~REFERENCE~~	~~M-002~~
GOAL	Identification of common misconfigurations.
RESULT	During the retest activities the previously mentioned vulnerability regarding the deletion of user's password does no longer exist.
DESCRIPTION	
During the rest activities it was found that the user's password is not affected by the previously mentioned vulnerability and therefore the issue can be marked as resolved.	
EVIDENCE	
N/A	

2.4.4 CLEAR-TEXT CREDENTIALS

REFERENCE	~~M-003~~ R-002
GOAL	Identification of security misconfigurations.
AFFECTED HOST	www.orlo.app (app.socialsignin.co.uk)
RESULT	During the retest it was found that it is not possible to retrieve user's password in cleartext from a password reset request. However, it was found that the user is not enforced to change the new generated password that has received during the "forgot password" action after successful login. Therefore, the previously mentioned vulnerability can be marked as partially solved. Customer has already been informed via email.
SEVERITY	RECOMMENDATION
LIKELYHOOD	N/A
EFFORT TO FIX	N/A

ISSUE DESCRIPTION
During the retest activities it was found that the application sends a random generated password in the user's email after a "forgot password" request. However, it was found that user can bypass the "change password" action after he/she login in with the random generated and can browse within the application normally. Therefore, user can keep using the random generated password which is displayed in plaintext in his/her email.
ISSUE EVIDENCE
N/A
REMEDIATION
Ensure that user is not able to use the application before change his/her password immediately after a forgot password action.

2.4.5 ANTI-BRUTE FORCE MECHANISMS BYPASS

~~REFERENCE~~	~~L 001~~
GOAL	Identification of security misconfigurations.
RESULT	During the retest activities it was found that it is not possible to conduct a brute-force or a dictionary based attack.

DESCRIPTION

During the retest activities it was found that the application enforces an anti-brute force mechanism correctly. As a result, an attacker cannot attempt to compromise an account by spraying different password combinations.

EVIDENCE

The following evidence shows the brute force mechanism implementation.

Request:

```
POST /user/login HTTP/1.1
Host: app.socialsignin.co.uk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: application/json, text/plain, */*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
Content-Length: 115
Origin: https://www.orlo.app
Connection: close
Referer: https://www.orlo.app/
{"email_address":"damian.papadamianou@bulletproof.co.uk","password":"kMb4ksdncC9C","long_exp
ire":true,"type":"web"}
```

Response:

```
HTTP/1.1 400 Bad Request
Date: Mon, 05 Oct 2020 13:58:52 GMT
Content-Type: application/json
Content-Length: 124
Connection: close
Server: Apache
SSI-BackendServer: ip-172-21-11-35
Access-Control-Allow-Origin: https://www.orlo.app
Access-Control-Expose-Headers: SSI-BackendServer, SSI-TraceId
Strict-Transport-Security: max-age=36000
Cache-Control: no-cache
SSI-TraceId: X3smmwlvu59lOqyzCMdmdAAAABI

{"error":1,"message":"There have been too many incorrect login attempts recently, please try
again later.","error_code":400}
```

2.4.6 HTML INJECTION

REFERENCE	L-002
GOAL	Identification of input validation issues.
AFFECTED HOST	www.orlo.app (app.socialsignin.co.uk)
RESULT	During the retest activities it was found that the application allows a user to inject special HTML characters.
SEVERITY	LOW
LIKELYHOOD	HIGH
EFFORT TO FIX	LOW

ISSUE DESCRIPTION

During the retest activities it was found that the application allows user input that contains HTML special characters. As a result, an attacker can inject HTML in order to affect the overall integrity of the application content.

ISSUE EVIDENCE

The following evidence shows that an attacker is able to inject HTML code.

The following evidence shows the injected set of characters (*html inject):*

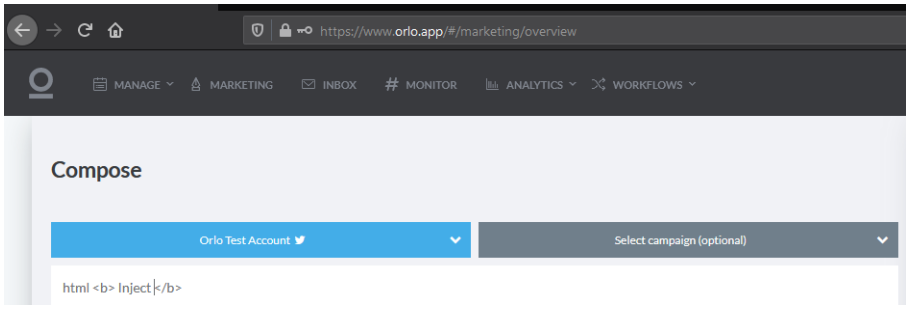

Figure 3: HTML Injection

The following evidence shows that the injected characters have been processed normally:

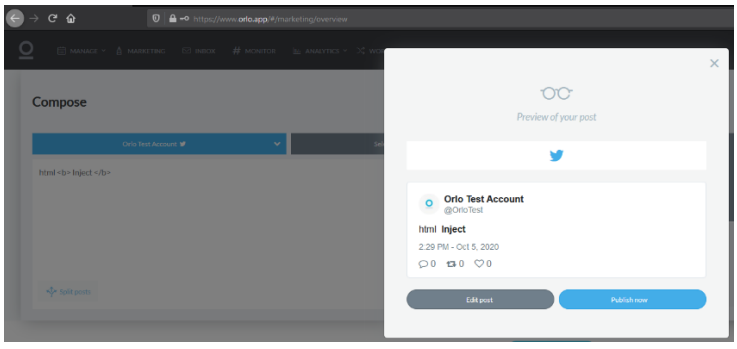

Figure 4: HTML Injection – Response

REMEDIATION

Any user input should be properly sanitised in order to prevent attacks, such as injection attacks.

2.4.7 INFORMATION DISCLOSURE

~~REFERENCE~~	~~R-001~~
GOAL	Identification of information leakage.
RESULT	During the retest activities it was found that the application leaks information through the HTTP response headers.

DESCRIPTION

During the retest activities it was found that the application do not leak information in the HTTP response headers.

EVIDENCE

The following evidence presents the HTTP response headers before our email communication with the customer:

Response snippet:

```
% curl -I https://app.socialsignin.co.uk
content-type: application/json
server: Apache
strict-transport-security: max-age=36000
status: 404 Not Found
cache-control: no-cache
ssi-traceid: X3xRdJUWVWlur4s@xGjfvgAAAAY
```

3. NEXT STEPS

We strongly recommend investigating and remediating all issues found throughout this penetration test. We have listed them in order of priority, with a justification for each vulnerability.

PRIORITY	REFERENCE	DESCRIPTION	REASON
1	L-002	HTML Injection	The application allows HTML to be inserted by a user.
2	R-002	Clear-Text Credentials	The user can bypass the change password page and can continue use the random generated password.

4. APPENDIX

4.1 CLEANUP

It is advised that the following account is removed:

- damian.papadamianou@bulletproof.co.uk

It is also recommended that any content added by this account be removed from the site.

T: 01438 532 900 E: contact@bulletproof.co.uk W: www.bulletproof.co.uk