Management response to Trustwave Penetration Test March 2023

To whom it may concern,

Lexer is pleased to provide you with its updated Penetration Test findings which were conducted by Trustwave in February 2023, and a remediation test performed in March 2023 ("**Test Report**").

Trustwave's Test Report found that Lexer's applications and underlying infrastructure adhered to "Best Practice" standards, and noted that Lexer's *"overall inherent security posture of the web application and external infrastructure [are] at a 'Best Practice/Informational' risk level."*

We are pleased that the Test Report has not found **any** issue which would incur a consequence rating (Insignificant to Catastrophic, as described in Appendix E of the Test Report).

Lexer welcomes this additional feedback on how it can continually improve the security of its infrastructure, and will consider the recommendations of Trustwave relating to "best practice" in its 2023/24 security roadmap.

Trustwave Finding			Lexer Management Response	
Risk	**Ref.**	**Weakness**	**Status**	**Comment**
Best Practice	DISC-1	Misconfiguration: Potentially Hijackable DNS Records	Remediated	Lexer has already addressed this issue in its remediation test.
Informational	APP-1	Insufficient Authorisation: Username Enumeration	No action required	This issue relates to the infrastructure of a third party, and has been noted for information only, as outside of the control of Lexer.
Best Practice	APP-2	Application Misconfiguration: Cookie without SameSite attribute	No immediate action required	Lexer will consider Trustwave's recommendations as part of its 2023/24 security roadmap.
Best Practice	INFRA-1	Best Practice: Lack of Security Headers	No immediate action required	Lexer will consider Trustwave's recommendations as part of its 2023/24 security roadmap.

Noting that the designation "Best Practice" has not been defined in the Test Report, we have confirmed with Trustwave that, for the purposes of their report, it means:

> *For those observations/shortcomings where we cannot ascertain the impact or likelihood (potentially due to the lack of visibility of the attack surface), but at the same time there are security best practices available, we usually mark it as "best practice".*

If you have any questions please email us at security@lexer.io.

Regards,

The Lexer Information Security Team

Enc: Trustwave Test Report

Trustwave

29 March 2023

Lexer Pty Ltd
86 Inkerman St, St Kilda VIC 3182

Re: Lexer Annual Penetration Test

As a part of Lexer’s ongoing security assurance, Lexer engaged Trustwave to perform an OSINT with attack surface discovery exercise, an application penetration test on the Lexer Hub web application and respective API endpoints as well as an infrastructure penetration test of the externally accessible subdomains and IP addresses. The purpose of this security assessment was to assess the security posture of the internet facing systems against common vulnerabilities and misconfigurations that could be leveraged by threat actors for the purpose of gaining unauthorised access to sensitive systems or data.

Trustwave web application testing methodology considers the following industry benchmarks and approaches:

- Open Source Security Testing Methodology Manual (OSSTMM) v3
- SANS/MITRE Common Weakness Enumeration (CWE) Top 25
- Open Web Application Security Project (OWASP) Top 10 Vulnerabilities
- Open Web Application Security Project (OWASP) API Security Top 10
- Web Application Security Consortium (WASC)

Trustwave performed the penetration test of the in-scope systems against the production environment in February 2023 and a remediation test in March 2023.

Lexer remediated all the security issues reported in the penetration test report in a timely and professional manner placing the overall inherent security posture of the web application and external infrastructure at a **‘Best Practice/Informational’** risk level.

Trustwave acknowledges all the cyber security initiatives Lexer continues to take in building a robust platform for its clients.

Regards,

Sarath Nair
Managing Consultant, SpiderLabs
Trustwave

This letter has been issued to Lexer upon their request.

Project Ref. PR-030581

By Jamie Eccleston, Coen Fox, Troy Driver

Lexer Annual Penetration Test Report

This document details the security posture of the Lexer Infrastructure and Application based on the findings identified by Trustwave during the Discovery and Annual Penetration Test performed in February 2023, and the remediation test performed in March 2023.

Summary

Trustwave conducted its annual penetration test on Lexer's systems which includes the assessment of Lexer's hub web application and external infrastructure. Trustwave also conducted a discovery exercise focusing on mapping out Lexer's internet attack surface. The purpose of the penetration tests was to assess the security posture of Lexer's application and infrastructure from the perspective of unauthenticated and authenticated users. The scope of the OSINT exercise was the entire Internet presence of Lexer. This included IP addresses, domains, subdomains, Lexer information on third-party products, leaked (intentionally or otherwise) internal information pertaining to Lexer, and employee email addresses.

Trustwave identified the Lexer application and external infrastructure to be generally secure. Prior to re-classification, Trustwave identified a User Enumeration vulnerability where attackers can verify if a username or email address exist within the web application. This was later re-classified to be a known and accepted issue by the third party authentication provider. Given that the issue lies within the infrastructure of the third-party provider and will not be remediated, the severity of this finding was changed from Low to Informational.

Trustwave found no potentially sensitive information about Lexer on the internet. Although prior to remediation, Trustwave identified a subdomain pointing to an AWS S3 bucket that may be susceptible to DNS hijacking.

Target Systems

- Internet Attack Surface of Lexer
- Lexer Application (hub.lexer.io)
- External Infrastructure

Risk Level

~~**Low**~~

Best Practice

Key Strengths

- Lexer's external infrastructure has minimal external footprint and attack surface.
- The Lexer application delegates file uploads and other input handling to AWS, greatly reducing the potential for Lexer's servers to be compromised through this attack vector.
- User controllable inputs to application functions are thoroughly sanitised server-side, mitigating attacks relying on stored or reflected user input.
- The application uses session tokens to uniquely verify users' sessions with a combination of Cross Site Request Forgery 'XSRF' tokens for sensitive functionality.
- Most systems and applications are up to date with the latest security patches.

Key Weaknesses (Best Practices)

- It is possible to enumerate existing email addresses registered on the web application.
- Identification of missing security headers which may aid exploitation of certain types of vulnerabilities.

Table of Contents

1 How to Read this Document

A one page 'cheat sheet' of this document

Summary

Detailed analysis of findings

Detailed Findings

What was tested

Appendix A – Assessed Targets

The project team and schedule

Appendix B – Project Schedule

Trustwave's test methodology

Appendix C – Test Methodology

Trustwave's risk methodology

Appendix D – Risk Assessment

2 Priority of Weakness

This section provides the priority of the findings identified during the penetration test. The priority is based on the rated risk for each security issue.

Phase 1 – Discovery Exercise

Risk	Ref.	Weakness
~~Low~~ Remediated	DISC-1	Misconfiguration: Potentially Hijackable DNS records

Phase 2 – Application Penetration Test

Risk	Ref.	Weakness
~~Low~~ **Informational**	APP-1	Insufficient Authentication: Username Enumeration
Best Practice	APP-2	Application Misconfiguration: Cookie without SameSite Attribute

Phase 2 – External Infrastructure Penetration Test

Risk	Ref.	Weakness
Best Practice	INFRA-1	Best Practice: Lack of Security Headers

3 Discovery Exercise Observations

Lexer engaged Trustwave to perform an Open Source Intelligence (OSINT) exercise during February 2023. The purpose of this engagement was to identify information in the public domain that could assist an adversary to further their objectives against Lexer. The OSINT exercise involved performing reconnaissance tasks to accurately determine Lexer's external attack surface, internet footprint, and potentially sensitive information unknowingly disclosed online.

The following report has been broken into sections based on the key objectives of the OSINT exercise:

1. Perform IP address and domain reconnaissance.
2. Identify potentially sensitive information inadvertently exposed in the public domain or on non-Lexer channels.
3. Identify DNS misconfigurations and subdomain hijacking issues.
4. Identify email addresses of Lexer employees searchable and verifiable from the internet.

This section details the recommendations made in response to the OSINT exercise performed.

This section provides a detailed description of the Discovery activities performed to gather information, the results and information gathered during these activities, and a link to any applicable recommendations.

Domain and IP Address Reconnaissance

Trustwave identified domain names and IP addresses belonging to Lexer as a starting point for conducting further activities including subdomain identification and the enumeration of publicly exposed services. The techniques used to identify domain names, subdomains, and IP addresses included:

- Searching Lexer's Autonomous Systems (AS) number for IP address ranges.
- Performing reverse 'whois' lookups using registrar email addresses and name.
- Performing reverse 'whois' lookups against IP addresses of Lexer assets.
- Performing subdomain enumeration techniques, including:
  - Scraping third party services for historical DNS records.
  - Running exhaustive DNS queries using wordlists of common subdomains
  - Feeding successful results from the previous two steps into "intelligent" subdomain mutation tools.
  - Re-running DNS queries against subdomains.
  - Querying Transport Layer Security (TLS) certificate transparency logs.
- Reviewing TLS certificates for alternative domain names.
- Searching within specific Internet footprint search engines.
- Using keywords from a Lexer provided "Prowler" output of an AWS Infrastructure scan for OSINT as well as subdomain and URL path brute forcing.

Results:

Trustwave identified 22 Top Level Domain (TLD) names potentially belonging to Lexer. The identified TLDs and IP addresses were then used in subdomain enumeration processes, resulting in the identification of 154 subdomains, 137 of which are valid and resolvable.

The Application Penetration Test and External Infrastructure Penetration Test assessed a total of 41 subdomains. Given this, out of the 137 resolvable subdomains, 97 subdomains were not tested during this engagement which may be candidates for future application and infrastructure tests.

Information relating to the discovered TLDs, subdomains, IP Addresses and email addresses can be found in the supplementary **Discovery Sheet – Lexer 2023.xslx** file.

Potentially Sensitive Information

Trustwave performed a series of internet search queries to identify potentially sensitive information pertaining to Lexer, both hosted on Lexer's infrastructure, and hosted on third-party services. The search queries included:

- Keywords containing each subdomain discovered belonging to all 3 valid TLDs found by Trustwave;
- Filetypes containing all the discovered subdomains within URLs; and
- Searching third-party services, such as GitHub, Stack Overflow, and Trello for mentions of Lexer as well as each discovered subdomains.

Results:

Trustwave observed that most results pointed to what appears to be Lexer's GitHub account Lexerdev (https://github.com/lexerdev). Another observation is that "tag.lexer.io" is included in repositories and commits to internet privacy and DNS blocklists. A number of documents were also available in the public domain hosted on Lexer's infrastructure, none of which were identified as sensitive.

Email Address Reconnaissance

Trustwave used multiple sources to gather employee names and email addresses for each domain name that was identified as being related to Lexer. The sources queried to harvest email addresses included email scraping services, social media platforms such as LinkedIn and search engine queries. A summary of the domain names where email addresses were able to be harvested, including the number of unique email addresses identified is shown in the below table.

Domain Name	Employee Names Collected	Email Addresses Collected	Validated Email Addresses
lexer.io	114	16	80

Results:

Trustwave was able to harvest employee names and email addresses during the discovery exercise. Part of Trustwave's methodology is to look for employees using their corporate email address to register on various online services and associate with the organisation on their LinkedIn accounts. Through analysis of the email addresses, Trustwave was able to infer that the naming convention used at Lexer is '*firstname.lastname@lexer.io*. Given this, Trustwave merged the collected employee names and verified them against the mail service provider, Gmail, with resulted in more than 80% of the total email addresses gathered.

DNS Misconfigurations and Subdomain Hijacking

Trustwave used the results of the domain/subdomain enumeration to perform manual and automated analysis of DNS records. The intent of the analysis was to identify misconfigurations which could be abused by malicious third parties.

Automated tools were used to scan all identified subdomains for DNS records which could result in a "Subdomain Takeover". The premise of a subdomain takeover is a record pointing to a service which is no longer in use; a third party is then able to claim an account on the service, and consequently control the content served by the vulnerable subdomain.

In addition to subdomain takeovers, Trustwave manually reviewed DNS records to identify stale records, which point to third party hosting providers. These misconfigurations cannot be directly abused to perform a takeover; however, they still present a potential security risk which could cause reputational damage to the organisation if a malicious third party were able to host malicious services on those resolved hosts.

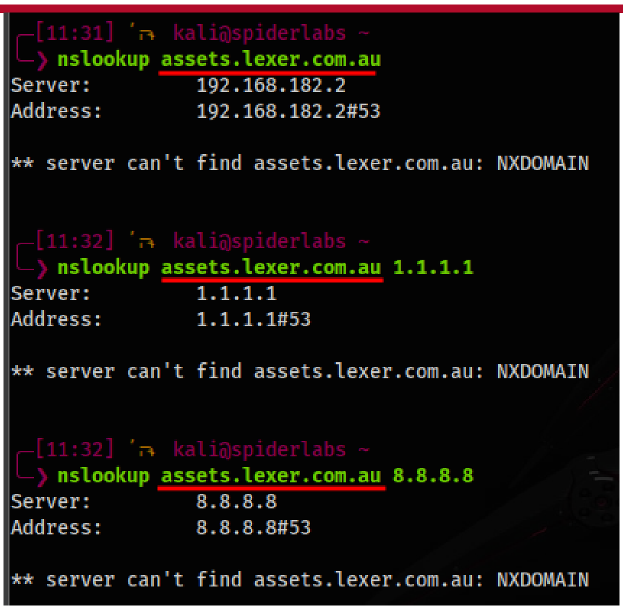
Results:

Trustwave identified one (1) potential subdomain hijacking issue, none of Trustwave attempted to exploit. These potential issues may materialise in the future if targeted by an attacker.

The recommendation below has been listed based on a priority of implementation: High, Medium, Low, or Very Low. This priority is based on Trustwave's understanding of the risk posed to Lexer and the specific evidence uncovered during the Discovery exercise:

DISC-1 Misconfiguration: Potentially Hijackable DNS records

Priority	**Recommendation**
~~Low~~ **Remediated**	In the time available for testing, Trustwave found one (1) potential hijackable subdomain or DNS record which were subdomains that pointed to AWS S3 buckets that no longer existed. Trustwave did not attempt to create an S3 bucket, take control or hijack the affected subdomain or DNS record as exploitation is not part of the Discovery exercise. However, the issue may be exploited by attackers in the future especially as new methodologies are discovered in combination with the constantly changing digital landscape or underlying infrastructure which the affected DNS record currently resolves to. Given this, Trustwave recommends that Lexer address and remove the following DNS record if not in use: • assets.lexer.com.au NOTE: Trustwave performed a remediation test on March 23, 2023, and found that the issue has been fixed. Below is a screenshot showing that the DNS record can no longer be resolved:



```
┌─[11:31] kali@spiderlabs ~
└─❯ nslookup assets.lexer.com.au
Server:         192.168.182.2
Address:        192.168.182.2#53

** server can't find assets.lexer.com.au: NXDOMAIN


┌─[11:32] kali@spiderlabs ~
└─❯ nslookup assets.lexer.com.au 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

** server can't find assets.lexer.com.au: NXDOMAIN


┌─[11:32] kali@spiderlabs ~
└─❯ nslookup assets.lexer.com.au 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

** server can't find assets.lexer.com.au: NXDOMAIN
```

4 Penetration Test Detailed Findings

4.1 Effective and Weak Security Controls

The table below provides a summary of the effective and weak security controls implemented in the Lexer Hub application:

Category	Lexer Hub Security Posture
Input Handling: All applications rely on inputs from a range of sources such as users, browsers, other applications via API. Improper input handling can lead to critical vulnerabilities as a result of the privileges with which input is often processed or executed by the application.	Effective Controls • The web application delegates file uploads and other input handling to AWS, greatly reducing the potential for Lexer's servers to be compromised through this attack vector. • User controllable inputs to application functions are thoroughly sanitised server-side, mitigating attacks relying on stored or reflected user input.
Authentication: Application security is reliant on the effective implementation of authentication controls. Insufficient authentication occurs when a web application permits an attacker to access content or functionality without having to properly authenticate.	Effective Controls • The web application requires user authentication to access all application pages and functionality; any user-specific functions the user can request will return 401 Unauthorised if no authentication is present.
Authorisation: While the 'authentication' function confirms a user's identity, it does not necessarily mean that the user should have full access to all content and functionality available in a given system. Insufficient authorisation procedures can allow an authenticated user – that is, a genuine user of a system – the ability to access data or functionality that they are not permitted to access.	Effective Controls • The web application uses session tokens to uniquely verify users' sessions with a combination of Cross Site Request Forgery 'XSRF' tokens for sensitive functionality.
Transport Layer Protection: The 'transport layer' refers to the delivery of content to and from the client and server. Insufficient transport layer protection may allow communication between the client and server to be exposed to untrusted third-parties, providing an attack vector to compromise a web application and/or obtain sensitive information.	Effective Controls • The web application enforces HTTPS encrypted transmission of sensitive data.
Information Leakage: Information leakage refers to a situation in which a system reveals internal – and potentially sensitive – data, often through error messages or incorrect system configuration. The data generally does not	Effective Controls • The web application generally does not disclose information if there are server-side errors in processing user requests.

present a ‘breach’, however it can often be used to further target subsequent attacks and thus introduces risk to the environment.	Weak Controls • However, the authentication API endpoint used for login consistently responds to registered email addresses faster than unregistered email addresses. This may assist a malicious attacker to compile a list of registered customer email addresses.
Application Misconfiguration: Application misconfigurations are often caused by unnecessary, default and sample features enabled by default. These default configurations if left enabled, may provide an avenue for attackers to bypass authentication methods, or gain access to system information.	Effective Controls • The system infrastructure and supporting components are updated with the latest security patches. Weak Controls • Several HTTP Security headers are missing or not set on some hosts.

4.2 Application Penetration Test

The following security issues were identified during the Application Penetration Test.

APP-1	**Insufficient Authentication: Username Enumeration**
Description	Application security is reliant on the effective implementation of authentication controls. Insufficient authentication processes that leak username information for example, allows an attacker to perform a targeted attack against the authentication mechanism. The Lexer Hub application responds differently when an existing email address is submitted compared to when an unregistered email address is submitted. This allows an attacker to perform a targeted attack against the enumerated users in order to attempt to gain unauthorised access to the application.
Proof of Concept	1. Navigate to the login page using a web interception proxy 2. Submit an unregistered email address to the application and note the response time of the request 3. Submit a registered email address to the application and note that the response time of the request **Affected systems:** • https://account.lexer.io/api/v1/authn Refer to appendix APPX-I for proof of concept screenshots.
Consequence	**Minor:** The disclosed accounts do not lead to direct compromise of the application but may assist an attacker in performing targeted attacks against application users such as password spraying and social engineering attacks. Successful password guesses and phishing attacks may allow an attacker to gain unauthorised access to the application and potentially, the internal network.
Likelihood	**Possible:** Tools are publicly available to aid in enumerating registered accounts in a short amount of time. However, as the application enforces a strong password policy, the likelihood of guessing the affected user’s password is decreased.
Risk	~~**Low**~~ **Informational** NOTE: Trustwave performed a remediation test on March 23, 2023, the issue remains but has been re-classified to be an ‘Informational’ finding since the issue lies within the infrastructure of the third-party provider. The third-party provider is aware of and will not remediate the issue.
Remediation	Configure the application such that there is no noticeable difference in response time for registered and unregistered users.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html#authentication-responses

APP-2 Application Misconfiguration: Cookie without SameSite Attribute

Description

Cookies are used by the Lexer Hub web application to uniquely identify an authorised user's application session. The Lexer Hub web application does not explicitly set the 'SameSite' flag on the 'JSESSIONID' cookie when sending the cookie within a HTTP response. This may make it possible for the cookie to be used in Cross Site Request Forgery attacks, though the attribute is set to 'Lax' by default in some modern browsers.

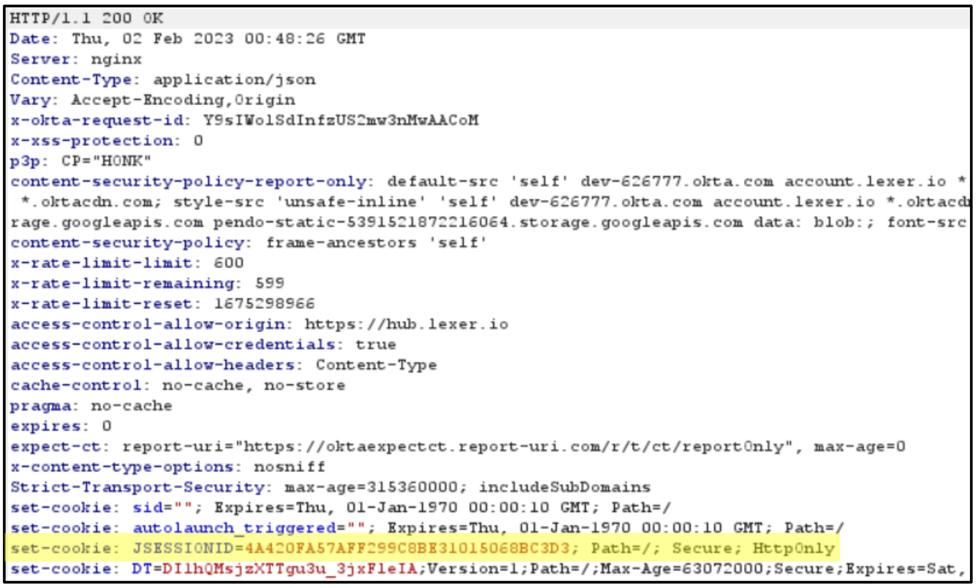
Proof of Concept

1. Authenticate to the Lexer Hub web application using a web browser with a web interception proxy.
2. Observe the lack of the 'SameSite' Attribute in the 'JSESSIONID' cookie in the application response.

Vulnerable path:

- https://account.lexer.io/api/v1/authn

Vulnerable cookie 'JSESSIONID' returned after successful authentication:



```
HTTP/1.1 200 OK
Date: Thu, 02 Feb 2023 00:48:26 GMT
Server: nginx
Content-Type: application/json
Vary: Accept-Encoding,Origin
x-okta-request-id: Y9sIWolSdInfzUS2mw3nMwAACoM
x-xss-protection: 0
p3p: CP="HONK"
content-security-policy-report-only: default-src 'self' dev-626777.okta.com account.lexer.io *
 *.oktacdn.com; style-src 'unsafe-inline' 'self' dev-626777.okta.com account.lexer.io *.oktacd
rage.googleapis.com pendo-static-5391521872216064.storage.googleapis.com data: blob:; font-src
content-security-policy: frame-ancestors 'self'
x-rate-limit-limit: 600
x-rate-limit-remaining: 599
x-rate-limit-reset: 1675298966
access-control-allow-origin: https://hub.lexer.io
access-control-allow-credentials: true
access-control-allow-headers: Content-Type
cache-control: no-cache, no-store
pragma: no-cache
expires: 0
expect-ct: report-uri="https://oktaexpectct.report-uri.com/r/t/ct/reportOnly", max-age=0
x-content-type-options: nosniff
Strict-Transport-Security: max-age=315360000; includeSubDomains
set-cookie: sid=""; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
set-cookie: autolaunch_triggered=""; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
set-cookie: JSESSIONID=4A420FA57AFF299C8BE31015068BC3D3; Path=/; Secure; HttpOnly
set-cookie: DT=DI1hQMsjzXTTgu3u_3jxFleIA;Version=1;Path=/;Max-Age=63072000;Secure;Expires=Sat,
```

Consequence

Moderate: An attacker could use the 'JSESSIONID' cookie in a CSRF attack to perform unauthorised actions on the Lexer Hub web application, under the victim's security context.

Likelihood

Rare: Exploitation of this security issue is a two-step process that requires an attacker to understand the Lexer Hub application's architecture to prepare a sensitive request, and then successfully coerce the client into clicking a link that will make that request, since the cookie has the 'HttpOnly' flag set. The Lexer Hub application appropriately implements CSRF tokens to prevent CSRF attacks on all sensitive functions; however, SameSite cookies are an important layer of defence. At the time of writing, Firefox and Safari, as well as their iOS counterparts, do not set SameSite appropriately by default, so it must be set explicitly.

Risk

Best Practice

Remediation	Configure the application to explicitly send the 'SameSite' attribute, set to 'Lax' for all sensitive application cookies.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite

4.3 External Infrastructure Penetration Test

The following security issues were identified during the external infrastructure penetration test.

INFRA-1 Best Practice: Lack of Security Headers

Description

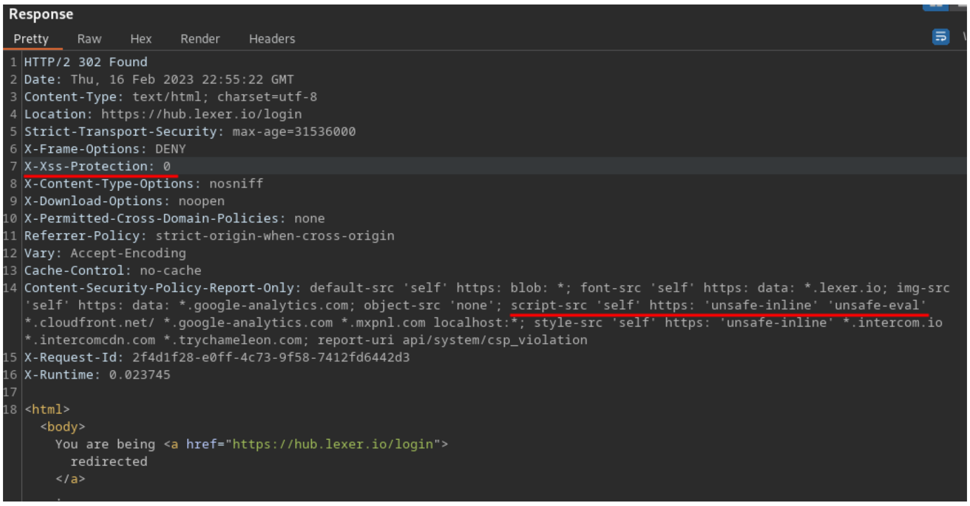
As web applications and services have become ubiquitous, numerous security enhancements have been added to enhance security within web applications. These features are typically implemented on the server side and are enabled through special HTTP headers. Enabling these headers provides additional security for the client-server communications and resilience to client-side attacks.

Trustwave identified that the following headers are not included in responses from the Lexer external hosts:

- **Strict Transport Security (HSTS)** policy informs a browser to only send all communications over HTTPS
- **Framing Protection Controls**, framing is allowed by default, if the application does not have a framing policy configured, it is possible to embed the application within an untrusted third-party domain

Proof of Concept

1. Submit a valid application request with a web interception proxy.
2. Observe the lack of security headers in the response HTTP headers.



```
HTTP/2 302 Found
Date: Thu, 16 Feb 2023 22:55:22 GMT
Content-Type: text/html; charset=utf-8
Location: https://hub.lexer.io/login
Strict-Transport-Security: max-age=31536000
X-Frame-Options: DENY
X-Xss-Protection: 0
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: strict-origin-when-cross-origin
Vary: Accept-Encoding
Cache-Control: no-cache
Content-Security-Policy-Report-Only: default-src 'self' https: blob: *; font-src 'self' https: data: *.lexer.io; img-src
'self' https: data: *.google-analytics.com; object-src 'none'; script-src 'self' https: 'unsafe-inline' 'unsafe-eval'
*.cloudfront.net/ *.google-analytics.com *.mxpnl.com localhost:*; style-src 'self' https: 'unsafe-inline' *.intercom.io
*.intercomcdn.com *.trychameleon.com; report-uri api/system/csp_violation
X-Request-Id: 2f4d1f28-e0ff-4c73-9f58-7412fd6442d3
X-Runtime: 0.023745

<html>
  <body>
    You are being <a href="https://hub.lexer.io/login">
      redirected
    </a>
```

The following letters correspond to hosts in the table below:

A. https://account.lexer.io/

B. https://clients.lexer.io/

C. https://hub.lexer.io/

D. https://hub2.lexer.io/

E. https://attributes-manager.camplexer.com/

F. https://nylas.lexer.io/

G. https://svg.lexer.io/

H. https://tag.lexer.io/

I. https://1password.lexer.io/

In the following table, X denotes the assessed web application missing the corresponding security header:

Security Header	A	B	C	D	E	F	G	H	I
Strict-Transport-Security					X	X	X	X	X
X-Frame-Options	X				X	X	X	X	
X-Xss-Protection (While allowing ‘script-src unsafe-inline’)		X	X	X					

Consequence

The lack of security headers in the Lexer external hosts may leave it vulnerable in certain attack scenarios which could lead to unauthorised access and/or interception of sensitive communications between the client and application.

This is a Best Practice recommendation and therefore does not have a consequence rating.

Likelihood

A malicious attacker must first coerce an application user with a valid session to browse to a third-party domain and inadvertently execute malicious content to retrieve information from the application.

This is a Best Practice recommendation and therefore does not have a likelihood rating.

Risk

Best Practice

Remediation

Implement the following security headers in the affected systems according to the principle of least privilege.

An example of some values that could be included in the headers is given below:

- Strict-Transport-Security: max-age=31536000; includeSubDomains
- X-Frame-Options: DENY
- X-Content-Type-Options: nosniff

References

https://owasp.org/www-project-secure-headers

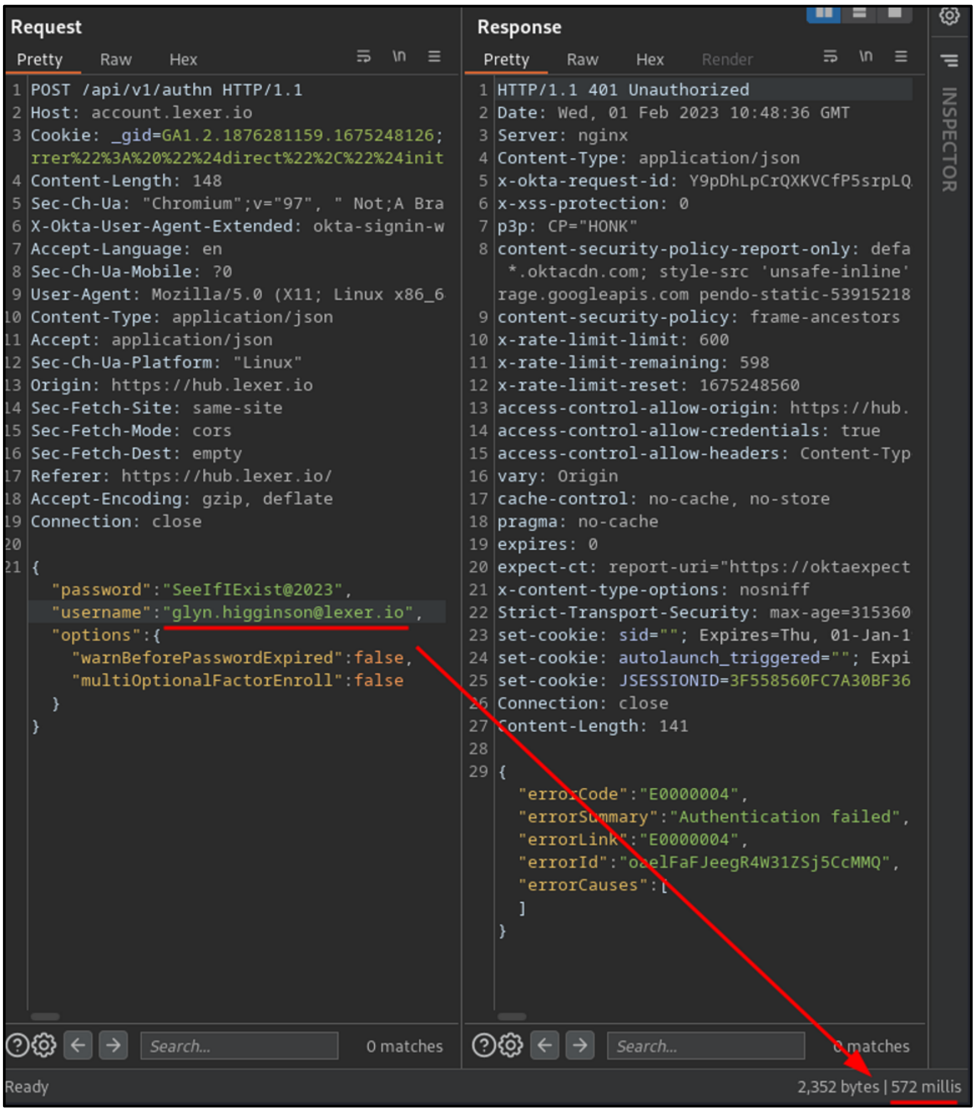
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers

Appendix A – Additional Details

APPX-I Insufficient Authentication: Username Enumeration

This section provides additional supporting information for the security issues in the Detailed Findings section - APP-1.

The following screenshot displays the response when an unregistered email address is submitted to the application, with the response time highlighted:

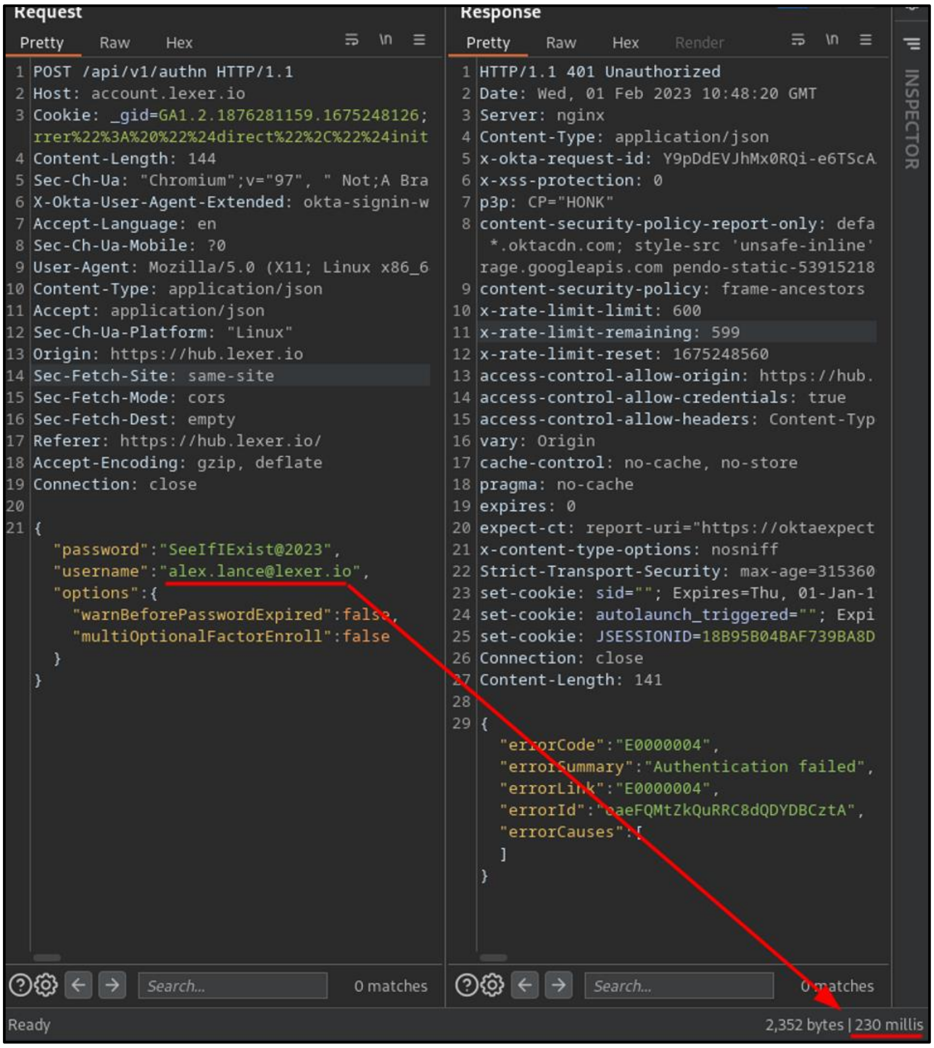


```
POST /api/v1/authn HTTP/1.1
Host: account.lexer.io
Cookie: _gid=GA1.2.1876281159.1675248126;
rrer%22%3A%20%22%24direct%22%2C%22%24init
Content-Length: 148
Sec-Ch-Ua: "Chromium";v="97", " Not;A Bra
X-Okta-User-Agent-Extended: okta-signin-w
Accept-Language: en
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_6
Content-Type: application/json
Accept: application/json
Sec-Ch-Ua-Platform: "Linux"
Origin: https://hub.lexer.io
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://hub.lexer.io/
Accept-Encoding: gzip, deflate
Connection: close

{
  "password":"SeeIfIExist@2023",
  "username":"glyn.higginson@lexer.io",
  "options":{
    "warnBeforePasswordExpired":false,
    "multiOptionalFactorEnroll":false
  }
}
```

```
HTTP/1.1 401 Unauthorized
Date: Wed, 01 Feb 2023 10:48:36 GMT
Server: nginx
Content-Type: application/json
x-okta-request-id: Y9pDhLpCrQXKVCfP5srpLQ
x-xss-protection: 0
p3p: CP="HONK"
content-security-policy-report-only: defa
 *.oktacdn.com; style-src 'unsafe-inline'
rage.googleapis.com pendo-static-53915218
content-security-policy: frame-ancestors
x-rate-limit-limit: 600
x-rate-limit-remaining: 598
x-rate-limit-reset: 1675248560
access-control-allow-origin: https://hub.
access-control-allow-credentials: true
access-control-allow-headers: Content-Typ
vary: Origin
cache-control: no-cache, no-store
pragma: no-cache
expires: 0
expect-ct: report-uri="https://oktaexpect
x-content-type-options: nosniff
Strict-Transport-Security: max-age=315360
set-cookie: sid=""; Expires=Thu, 01-Jan-1
set-cookie: autolaunch_triggered=""; Expi
set-cookie: JSESSIONID=3F558560FC7A30BF36
Connection: close
Content-Length: 141

{
  "errorCode":"E0000004",
  "errorSummary":"Authentication failed",
  "errorLink":"E0000004",
  "errorId":"oaelFaFJeegR4W31ZSj5CcMMQ",
  "errorCauses":[
  ]
}
```

2,352 bytes | 572 millis

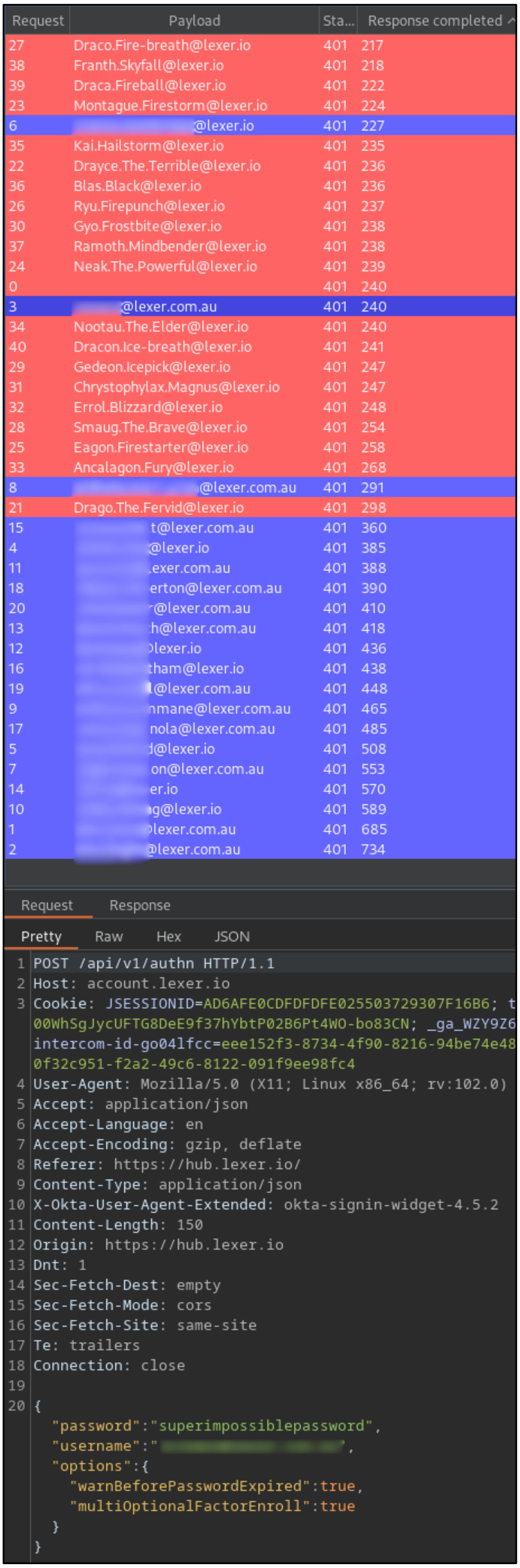
The following screenshot displays the response when a registered email address is submitted to the application, with the shorter response time highlighted:



```
POST /api/v1/authn HTTP/1.1
Host: account.lexer.io
Cookie: _gid=GA1.2.1876281159.1675248126;
rrer%22%3A%20%22%24direct%22%2C%22%24init
Content-Length: 144
Sec-Ch-Ua: "Chromium";v="97", " Not;A Bra
X-Okta-User-Agent-Extended: okta-signin-w
Accept-Language: en
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_6
Content-Type: application/json
Accept: application/json
Sec-Ch-Ua-Platform: "Linux"
Origin: https://hub.lexer.io
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://hub.lexer.io/
Accept-Encoding: gzip, deflate
Connection: close

{
  "password":"SeeIfIExist@2023",
  "username":"alex.lance@lexer.io",
  "options":{
    "warnBeforePasswordExpired":false,
    "multiOptionalFactorEnroll":false
  }
}
```

```
HTTP/1.1 401 Unauthorized
Date: Wed, 01 Feb 2023 10:48:20 GMT
Server: nginx
Content-Type: application/json
x-okta-request-id: Y9pDdEVJhMx0RQi-e6TScA
x-xss-protection: 0
p3p: CP="HONK"
content-security-policy-report-only: defa
 *.oktacdn.com; style-src 'unsafe-inline'
rage.googleapis.com pendo-static-53915218
content-security-policy: frame-ancestors
x-rate-limit-limit: 600
x-rate-limit-remaining: 599
x-rate-limit-reset: 1675248560
access-control-allow-origin: https://hub.
access-control-allow-credentials: true
access-control-allow-headers: Content-Typ
vary: Origin
cache-control: no-cache, no-store
pragma: no-cache
expires: 0
expect-ct: report-uri="https://oktaexpect
x-content-type-options: nosniff
Strict-Transport-Security: max-age=315360
set-cookie: sid=""; Expires=Thu, 01-Jan-1
set-cookie: autolaunch_triggered=""; Expi
set-cookie: JSESSIONID=18B95B04BAF739BA8D
Connection: close
Content-Length: 141

{
  "errorCode":"E0000004",
  "errorSummary":"Authentication failed",
  "errorLink":"E0000004",
  "errorId":"oaeFQMtZkQuRRC8dQDYDBCztA",
  "errorCauses":[
  ]
}
```

Below is a screenshot taken during the remediation test on March 23, 2023, showing that the issue still persists. The test was conducted with a list of valid and invalid users. The valid users are highlighted in blue and non-existing users highlighted in red.



Request	Payload	Sta...	Response completed ^
27	Draco.Fire-breath@lexer.io	401	217
38	Franth.Skyfall@lexer.io	401	218
39	Draca.Fireball@lexer.io	401	222
23	Montague.Firestorm@lexer.io	401	224
6	[redacted]@lexer.io	401	227
35	Kai.Hailstorm@lexer.io	401	235
22	Drayce.The.Terrible@lexer.io	401	236
36	Blas.Black@lexer.io	401	236
26	Ryu.Firepunch@lexer.io	401	237
30	Gyo.Frostbite@lexer.io	401	238
37	Ramoth.Mindbender@lexer.io	401	238
24	Neak.The.Powerful@lexer.io	401	239
0		401	240
3	[redacted]@lexer.com.au	401	240
34	Nootau.The.Elder@lexer.io	401	240
40	Dracon.Ice-breath@lexer.io	401	241
29	Gedeon.Icepick@lexer.io	401	247
31	Chrystophylax.Magnus@lexer.io	401	247
32	Errol.Blizzard@lexer.io	401	248
28	Smaug.The.Brave@lexer.io	401	254
25	Eagon.Firestarter@lexer.io	401	258
33	Ancalagon.Fury@lexer.io	401	268
8	[redacted]@lexer.com.au	401	291
21	Drago.The.Fervid@lexer.io	401	298
15	[redacted]t@lexer.com.au	401	360
4	[redacted]@lexer.io	401	385
11	[redacted]exer.com.au	401	388
18	[redacted]erton@lexer.com.au	401	390
20	[redacted]@lexer.com.au	401	410
13	[redacted]h@lexer.com.au	401	418
12	[redacted]lexer.io	401	436
16	[redacted]tham@lexer.io	401	438
19	[redacted]@lexer.com.au	401	448
9	[redacted]nmane@lexer.com.au	401	465
17	[redacted]nola@lexer.com.au	401	485
5	[redacted]d@lexer.io	401	508
7	[redacted]on@lexer.com.au	401	553
14	[redacted]er.io	401	570
10	[redacted]g@lexer.io	401	589
1	[redacted]lexer.com.au	401	685
2	[redacted]@lexer.com.au	401	734

```
POST /api/v1/authn HTTP/1.1
Host: account.lexer.io
Cookie: JSESSIONID=AD6AFE0CDFDFDFE025503729307F16B6; t
00WhSgJycUFTG8DeE9f37hYbtP02B6Pt4WO-bo83CN; _ga_WZY9Z6
intercom-id-go04lfcc=eee152f3-8734-4f90-8216-94be74e48
0f32c951-f2a2-49c6-8122-091f9ee98fc4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Accept: application/json
Accept-Language: en
Accept-Encoding: gzip, deflate
Referer: https://hub.lexer.io/
Content-Type: application/json
X-Okta-User-Agent-Extended: okta-signin-widget-4.5.2
Content-Length: 150
Origin: https://hub.lexer.io
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers
Connection: close

{
  "password":"superimpossiblepassword",
  "username":"[redacted]",
  "options":{
    "warnBeforePasswordExpired":true,
    "multiOptionalFactorEnroll":true
  }
}
```

Appendix B – Assessed Targets

As part of Lexer security assurance process, the following systems were assessed to determine the security posture of the Infrastructure.

- Phase 1 – Discovery Exercise
- Phase 2 – Application Penetration Test
  - hub.lexer.io
  - api.lexer.io
- Phase 2 – External Infrastructure Penetration Test
  - hub.lexer.io
  - account.lexer.io
  - api.lexer.io
  - staging.api.lexer.io
  - tag.lexer.io
  - track.lexer.io
  - au.transfer.lexer.io
  - us.transfer.lexer.io
  - au.sftp.lexer.io
  - us.sftp.lexer.io
  - au-cdp-es-009.camplexer.com
  - us-cdp-es-009.camplexer.com
  - 1password.lexer.io
  - clients.lexer.io
  - fb.lexer.io
  - fonts.lexer.io
  - hub2.lexer.io
  - nylas.lexer.io
  - redir.lexer.io
  - sexy-asset.lexer.io
  - sexy.lexer.io
  - source-assets.lexer.io
  - svg.lexer.io
  - twitter.lexer.io
  - webhooks.lexer.io
  - api-test.camplexer.com
  - attributes-manager.camplexer.com
  - au-identity-history-staging.camplexer.com

- au-identity-history.camplexer.com
- beta-facebook-webhook.camplexer.com
- docker.camplexer.com
- hot-warm-dashboard.ec2.camplexer.com
- lexer-database-1.ec2.camplexer.com
- lexer-enrichment.ec2.camplexer.com
- lexer-gateway.ec2.camplexer.com
- lexer-manager-1.ec2.camplexer.com
- lexer-staging-az.ec2.camplexer.com
- lexer-staging.ec2.camplexer.com
- lexer-website.ec2.camplexer.com
- lexer-worker-1-processing.ec2.camplexer.com
- wallboard.ec2.camplexer.com

Appendix C – Project Schedule

The following is the Trustwave security assessment schedule and roles and responsibilities for this engagement:

Date	Name	Role and Responsibility
1 Feb 2023 – 17 Feb 2023	Sarath Nair	Project Management
1 Feb 2023 – 15 Feb 2023	Jamie Eccleston Coen Fox Troy Driver	Technical Security Testing
16 Feb 2023	Zak Willsallen	Quality Assurance

Appendix D – Test Methodology

Application Testing – Test Cases

Trustwave has developed an application testing methodology that can be adapted to a range of security testing targets and with consideration of a range of industry leading benchmarks and approaches:

- Open Source Security Testing Methodology Manual (OSSTMM) v3
- SANS/MITRE Common Weakness Enumeration (CWE) Top 25
- Open Web Application Security Project (OWASP) Top 10 Vulnerabilities
- Open Web Application Security Project (OWASP) API Security Top 10
- Web Application Security Consortium (WASC)

Through building our methodology around Weaknesses rather than Attacks, we can ensure that the methodology remains relevant for a broad spectrum of system types.

We conduct our testing using a structured approach. Our testing process involves initial application familiarisation – that is, getting a thorough understanding of how the system works, how the security elements are intended to operate, and the key business logic underpinning any core transactional functionality – followed by in-depth and comprehensive assessment of the technology itself.

The test cases described below are used as a starting point for response and behaviour analysis, with the responses then used to guide subsequent phases of analysis and attack.

Our core application security testing model is based around the WASC Threat Classification view of Weaknesses. This approach allows for the key issues with web applications to be analysed, while ensuring that an 'all threats' approach is taken as to how that weakness could arise.

Ref.	Weakness	OWASP Top 10 X-Ref[1]
AW1	Application/Server Misconfiguration	2021-A5 – Security Misconfiguration 2021-A6 – Vulnerable and Outdated Components 2019-API7 – Security Misconfiguration
AW2	Directory Indexing	2021-A5 – Security Misconfiguration 2019-API7 – Security Misconfiguration
AW3	Improper Filesystem Permission	2021-A1 – Broken Access Control 2019-API1 – Broken Object Level Authorization 2019-API5 – Broken Function Level Authorization
AW4	Improper Input Handling	2021-A3 – Injection 2021-A5 – Security Misconfigurations 2021-A8 – Software and Data Integrity Failures 2019-API8 - Injection

AW5	Improper Output Handling	2021-A3 – Injection 2013-A10 – Unvalidated Redirects and Forwards 2019-API8 - Injection
AW6	Information Leakage	2021-A2 – Cryptographic Failures 2019-API3 – Excessive Data Exposure
AW7	Insecure Indexing	2021-A5 – Security Misconfiguration 2019-API7 – Security Misconfiguration
AW8	Insufficient Anti-automation	2021-A7 – Identification and Authentication Failures 2021-A5 – Security Misconfiguration 2019-API2 – Broken User Authentication 2019-API7 – Security Misconfiguration 2019-API4 – Lack of Resource & Rate limiting
AW9	Insufficient Authentication	2021-A7 – Identification and Authentication Failures 2019-API2 – Broken User Authentication
AW10	Insufficient Authorisation	2021-A1 – Broken Access Control 2021-A10 – Server-Side Request Forgery 2019-API1 – Broken Object Level Authorization 2019-API5 – Broken Function Level Authorization 2019-API6 – Mass Assignment
AW11	Password Circumvention	2021-A7 – Identification and Authentication Failures 2019-API2 – Broken User Authentication
AW12	Insufficient Process Validation	-
AW13	Insufficient Session Expiration	2021-A7 – Identification and Authentication Failures 2019-API2 – Broken User Authentication
AW14	Insufficient Transport Layer Protection	2021-A5 – Security Misconfiguration 2021-A6 – Vulnerable and Outdated Components 2019-API7 – Security Misconfiguration
AW15	Insufficient Auditing and Logging	2021-A9 – Security Logging and Monitoring Failures 2019-API10 – Insufficient Logging & Monitoring

Infrastructure Testing – Test Cases

Infrastructure security testing involves specialist consultants attempting to compromise a target system using the same techniques commonly used by malicious attackers, focused on infrastructure components such as servers, operating systems, network and security devices.

Infrastructure penetration tests are generally combined with application tests due to the significant prevalence of application level vulnerabilities and compromises originating from this source. However, infrastructure level penetration tests and vulnerability scans continue to be of value to identify misconfiguration of devices, out of date components and missing patches.

Our infrastructure security assessment process uses a ‘drop in’ scanning system, and runs a series of scans to identify key infrastructure security issues as detailed in the test cases below. Based on the data identified from these scans, additional testing activities may be discussed with the client to provide concrete demonstration of vulnerability and removal of false positives.

Ref.	Weakness
IW1	Software Flaws
IW2	System Misconfiguration (Servers)
IW3	System Misconfiguration (Security Devices)
IW4	Information Leakage

This usually follows the following process:

- **Network Discovery**: The purpose of this step is to discover and map out the local infrastructure of the target network. At the end of the network discovery, the penetration tester should have a basic layout of the local network infrastructure.
- **Target Identification**: This step aims to identify a host of interest. This is usually a specific IP range, or a single host/server with many available open ports and corresponding services. At the completion of the target identification step, the penetration tester would have identified a specific target that is most likely to allow penetration of the target network. This may sometimes include additional infrastructure, such additional subnets, that were discovered during the detailed assessment and analysis.
- **Vulnerability Assessment**: This step includes detailed assessment and analysis of the security posture of the identified target. This includes assessing and analysing the services and software packages running on the identified network, and vulnerabilities that are commonly found on them.
- **Vulnerability Exploitation**: The step requires that the penetration tester perform manual verifications of the vulnerabilities that are commonly found on the available services on the target system. This usually includes attempts to bypass security controls, and the lack of, to perform unauthorised and most often unauthenticated transactions with the vulnerable services identified in the previous step.
- **Network Penetration**: Successful exploitation of the identified vulnerabilities will allow unauthorised penetration of the local network infrastructure and subsequent privilege escalation activities to access sensitive data and functionality.

Security Assessment Toolset

Security assessment tools are software applications that are designed to assist in identification of security vulnerabilities, reducing the time and effort to execute repeat processes. The following tools were used during the security assessment:

- Nuclei Vulnerability Scanner
- Burp Suite Pro web interception proxy
- Nessus Professional vulnerability scanner
- Nmap network security scanner
- Metasploit exploitation toolkit
- Wireshark network analysis tool
- Nikto web application vulnerability scanner
- Sqlmap automated SQL injection auditing tool
- SSLScan SSL configuration scanner
- Recursebuster directory brute forcing tool

Time Boxing

Many applications would require an unfeasibly large amount of testing to provide coverage of all functions within the application with respect to all user types and the permutations of such users and access. This is particularly the case for systems with a high number of user types and/or privilege levels (as testing every permutation of one account's ability to interact with every other account can create hundreds, or thousands, of such permutations).

As a result, most tests are effectively "time boxed", which means that a set amount of time is allocated for testing based on the assessed risk presented by the application and the budget available, and within that time, test tasks are prioritised based on the areas of highest risk – both the most likely vulnerabilities to exist; and those that would cause the greatest harm.

Constraints

The environment provisioned for the security assessment will influence the results of the test. Where a fragile and sensitive environment is used and where network access controls are present, it may be necessary to take a 'gentler' approach to the test with a corresponding reduction in the level of coverage able to be achieved in a certain time period.

Appendix E – Risk Assessment

The ISO (International Organisation of Standardisation) 31000 series is a family of risk management standards used widely within various industries as a guideline to internal or external audit programmes. The security assessment adopts the ISO 31000 risk assessment approach, incorporating risk assessment concepts from the MITRE organisations. These form the risk ratings assessed in this report. The following tables provide description of the likelihood, consequence and resulting risk rating used in this security assessment.

The interpretation of the likelihood of an event occurring is described as per below:

Likelihood Rating	Interpretation
Almost certain	The event is expected to occur. (e.g. 1 incident every month)
Likely	The event will probably occur. (e.g. 1 incident every 6 months)
Possible	The event should occur at some time. (e.g. 1 incident every year)
Unlikely	The event could occur at some time. (e.g. 1 incident every 2 years)
Rare	The event may occur only in exceptional circumstances. (e.g. 1 incident every 5 or more years)

Trustwave considers the following as contributing factors to the likelihood of an event occurring.

- The **value** of assets contained within the vulnerable system
  E.g. Credit card details or dummy test data
- The **skills** required to successfully exploit the vulnerable system using the vulnerability identified
- The availability of **exploits** on the public domain
- The **complexity** of the exploit
- The **level of access** on the vulnerable system required to exploit the security issue
  E.g. Privileged administrative user or anonymous user

The interpretation of the consequence of an event occurring is described as per below:

Consequence Rating	Sample Interpretation
Insignificant	Little disruption to the user community. Technologies in use will require little/no effort to change. Isolated complaint from individual stakeholder able to be managed via business as usual operations.
Minor	Minor disruption to user community. The ability to provide the required service is impaired. Complaints from key stakeholder requiring management attention.
Moderate	Some inconvenience to the user community. The ability to provide a service is severely compromised. Moderate effort required to implement an alternative solution. Public criticism from key stakeholders regarding the organisation's services or activities.
Major	Noticeable impact on user community. Some core services unavailable. Potential for serious distress or minor injury. Sustained criticism from majority of key stakeholders on suitability of organisation in its current form.
Catastrophic	Community unable to function without significant support. Key technologies no longer available and no viable alternative exists. Potential for major injury or fatalities. Irreparable damage to relationships with key stakeholders and potential for organisation to cease operating in current form.

The resultant risk rating is detailed in the following risk matrix:

	Rare	Unlikely	Possible	Likely	Almost Certain
Insignificant	Very Low	Very Low	Very Low	Low	Low
Minor	Very Low	Low	Low	Low	Low
Moderate	Low	Medium	Medium	Medium	Medium
Major	Medium	Medium	High	High	High
Catastrophic	High	High	Extreme	Extreme	Extreme

Appendix F – Revision History

Version	Date	Name	Revision Comment
0.1	14 February 2023	Jamie Eccleston Coen Fox Troy Driver	Initial report draft
0.2	16 February 2023	Zak Willsallen	Internal report review
0.3	17 February 2023	Sarath Nair	Client report release
0.4	27 March 2023	Troy Driver	Remediation Test
1.0	29 March 2023	Sarath Nair	Client report release