Gem Software Security Assessment

Gem

Version 1.0 – February 16, 2026

Prepared By
Samuel Gabrielle Malijan
Carl Jason Mangio

Prepared For
David Dold
Yi-An Lai

1 Executive Summary

Synopsis

During the period of February 2nd and February 6th, 2026, Gem engaged NCC Group to conduct a security assessment of the Gem Web Application and Browser Extension and External Network Infrastructure. The Gem Web application, and browser extension, is a recruiting automation and analytics solution. Users add prospective candidate data into Gem, including resume files. They then use Gem to send emails to engage candidates to apply for jobs. Email sending functionality leverages Google Mail accounts which are authenticated using OAuth. Candidate engagement activity and statistics are tracked and presented in the Gem UI. All major operations are performed using a GraphQL-based API.

Scope

NCC Group's evaluation included:

- **Gem Web Application and Browser Extension**: Provides talent recruitment services. Their software tracks and coordinates recruiting data and candidates.
  - https://www.gem.com
- **External Network**
  - gem.com

Testing was performed on the production version of the application hosted on https://gem.com/.

Limitations

There were no limitations during the testing and NCC Group was able to evaluate all components within the endpoints and platforms.

Key Findings

The assessment uncovered informational risk application flaws. The most notable findings were:

External Network The assessment revealed no significant security gaps or notable weaknesses in the external network infrastructure. The host was found to only expose HTTPS service and the configuration of service within the network was found to be robust and aligned with security best practices. With only a single service was exposed, the external attack surface was limited.

Web

No significant issues were found during the web application and browser extension assessment. Three informational-level issues were identified during the assessment, which pose minimal risk to the platform. However, the issues have been raised as part of a comprehensive defense-in-depth strategy.

Strategic Recommendations

General Application Hardening A majority of the identified findings were determined to pose an informational to low overall risk to the organization. Nevertheless, NCC Group recommends that all findings are reviewed and addressed in order to bring the production application environment in line with security best practices. It is important to recognize that even low risk issues can be exploited in combination with other issues as part of a wider attack which seeks to compromise an environment or application. In addition, resolving lower risk issues can have the dual benefit of reducing the attractiveness of systems to opportunistic attackers as well as enhancing the overall security posture of the platform.

External Network Continue to maintain the current security practices and remain vigilant in identifying and mitigating emerging threats. Regular security assessments and audits should be conducted to ensure ongoing compliance with industry standards and to proactively address potential vulnerabilities. Additionally, staying informed about the latest security trends and best practices will be crucial in maintaining a robust security posture.

2 Dashboard

Target Data

Name	Gem Software
Type	Web Application, External Network
Platforms	AWS, Heroku
Environment	Production

Engagement Data

Type	Web Application Security Assessment, External Network Security Assessment
Method	White-Box
Dates	2026-02-02 to 2026-02-06
Consultants	2
Level of Effort	8 person-days

Targets

External Network	gem.com
Web Application	https://www.gem.com

Finding Breakdown

Critical issues	0
High issues	0
Medium issues	0
Low issues	0
Informational issues	3
Total issues	**3**

Category Breakdown

Other	1
Session Management	1
Uncategorized	1

Critical High Medium Low Informational

3 Table of Findings

For each finding, NCC Group uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors.

Title	Status	ID	Risk
Session Handling and Timeout	New	E2C	Info
Automated Abuse Protections	Reported	TVA	Info
Insecure Entropy Identifier	Reported	7EA	Info

4 Finding Details

Info

Session Handling and Timeout

Overall Risk	Informational	**Finding ID**	NCC-E030222-E2C
Impact	Low	**Component**	Gem Web Application and Browser Extension Security Assessment
Exploitability	Low	**Category**	Session Management
		Status	New

Impact

Compromised session tokens will remain valid until specifically invalidated by the application.

Description

The Gem web application expires user sessions for slightly more than a month. The screenshot below displays the lifetime of the session:

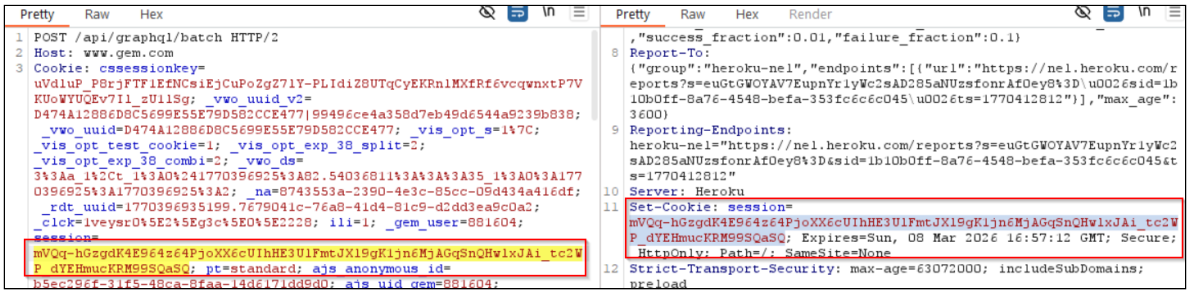

Figure 1: Lifetime of Session Token

Additionally, the application allows multiple concurrent sessions (e.g. from different devices or browsers) to be active at the same time. Below is a snippet of how two active sessions exist between two different browsers:

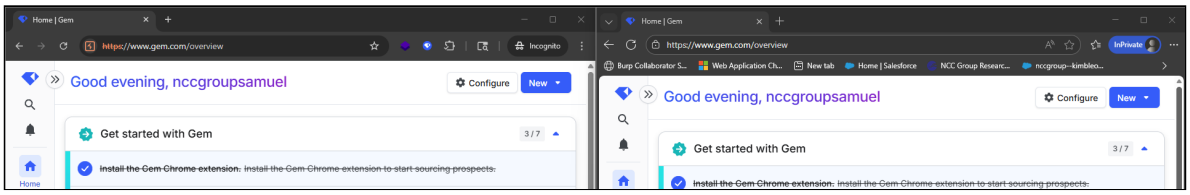

Figure 2: Concurrent Logins - Two Different Sessions from different Browsers

Users are able to access multiple sessions for the same account while the application lacks the ability to manage these sessions. Compromised users will remain unaware of these additional sessions. Additional sessions are not able to be terminated by the compromised user.

Many standards organizations such as PCI, OWASP, and NIST recommend extremely short timeouts (under an hour) before inactive user sessions are forcibly expired. A short timeout is argued to be a protection against account compromise in case a user's session token is leaked. However, there are few scenarios where session token compromise is likely that are also protected by a short timeout. The most commonly considered scenario (physical compromise of a user's device) is not one which a web application can reasonably protect against, even if extremely short timeouts are implemented.

The drawback of session invalidation is that it encourages users to use short passwords and to enter passwords without verifying the application's domain. For this reason, many companies make a choice not to expire user sessions without some evidence that the session is compromised. Instead, effort is shifted to alternative account protections which have real-world evidence of effectiveness[1], such as multi-factor authentication and proactive monitoring for evidence of token compromise. For example, a site might check the user's IP address and force a new login if the geolocation of the IP address has changed.

Recommendation

NCC Group recommends that most applications should set a reasonable session timeout that meets the standard followed by the organization. Session timeouts should not generally be shorter than one day (24 hours) unless mandated by an external standards organization. For applications which do not contain critically-sensitive user data or functionality, timeouts between one week and one month are reasonable. The session timeout may be increased or removed if the application implements strong account takeover (ATO) protections such as mandatory multi-factor authentication, proactive detection for ATO, and user visibility and management of sessions.

NCC Group does not recommend implementing any change which forces users to only have a single active session. Accessing an application across multiple devices or browsers is a common scenario which does not create a security risk for most web applications.

Reproduction Steps

1. Login with the account of your choice on a browser.
2. Login the previously logged in account on a different browser.
3. Observe that the session is not invalidated for both sessions.

Location

- www.gem.com

1. See *Account protections - A Google Perspective* by Elie Bursztein

Info

Automated Abuse Protections

Overall Risk	Informational	**Finding ID**	NCC-E030222-TVA
Impact	None	**Component**	Gem Web Application and Browser Extension Security Assessment
Exploitability	None	**Category**	Other
		Status	Reported

Impact

An attacker can more easily conduct automated attacks against the web services which may result in degraded service or enable spam and abuse.

Description

It was observed that the Gem GraphQL web service does not implement abuse protections such as rate limiting. Rate limiting prevents an attacker from exhausting hosted resources for the endpoint server, which could in some circumstances lead to a denial-of-service condition, or can result in increased operational costs for maintaining and scaling the API infrastructure. In the screenshot below, it shows that 1000 requests were sent in a short amount of time and were not rate limited.

Request	Payload	Status code	Response c...	Response received	Length
1126	..%c0%af..%c0%af..%c0%af..%c0%af.....	200	318	318	4887
1125	..%c0%af..%c0%af..%c0%af..%c0%afre...	200	353	353	4887
1124	..%c0%af..%c0%af..%c0%afrequireme...	200	357	357	4887
1123	..%c0%af..%c0%afrequirements.txt	200	359	359	4887
1122	..%c0%afrequirements.txt	200	332	332	4887
1121	..%c0%2f..%c0%2f..%c0%2f..%c0%2f.....	200	344	344	4887
1120	..%c0%2f..%c0%2f..%c0%2f..%c0%2f.....	200	302	302	4887
1119	..%c0%2f..%c0%2f..%c0%2f..%c0%2f.....	200	306	306	4887
1118	..%c0%2f..%c0%2f..%c0%2f..%c0%2fre...	200	323	323	4887
1117	..%c0%2f..%c0%2f..%c0%2frequireme...	200	308	308	4887
1116	..%c0%2f..%c0%2frequirements.txt	200	341	341	4887
1115	..%c0%2frequirements.txt	200	334	334	4887
1114	..%2f..%2f..%2f..%2f..%2f..%2f..%2freq...	200	333	331	4887
1113	..%2f..%2f..%2f..%2f..%2f..%2frequirem...	200	326	326	4887
1112	..%2f..%2f..%2f..%2f..%2frequirements....	200	331	331	4887
1111	..%2f..%2f..%2f..%2frequirements.txt	200	297	297	4879
1110	..%2f..%2f..%2frequirements.txt	200	308	308	4879
1109	..%2f..%2frequirements.txt	200	297	297	4879

Figure 3: No Rate Limiting

As indicated by the example HTTP response below, there was no rate limiting protection mechanism (or header) observed.

```
HTTP/2 200 OK
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://www.gem.com
Content-Security-Policy: ----snipped CSP policy----
Content-Type: application/json
Date: Tue, 03 Feb 2026 11:54:21 GMT
```

```
Nel: {"report_to":"heroku-nel","response_headers":["Via"],"max_age":3600,"success_fraction":
↳ 0.01,"failure_fraction":0.1}
Report-To: {"group":"heroku-nel","endpoints":[{"url":"https://nel.heroku.com/reports?
↳ s=ua6CbYt1q%2FZ51ZmqkRmCdr3wu%2BV6%2Bohi36cFBXqYa2E%3D\u0026sid=1b10b0ff-8a76-4548-
↳ befa-353fc6c6c045\u0026ts=1770724461"}],"max_age":3600}
Reporting-Endpoints: heroku-nel="https://nel.heroku.com/reports?
↳ s=ua6CbYt1q%2FZ51ZmqkRmCdr3wu%2BV6%2Bohi36cFBXqYa2E%3D&sid=1b10b0ff-8a76-4548-
↳ befa-353fc6c6c045&ts=1770724461"
Server: Heroku
Set-Cookie: ---snipped set-cookie header---
Vary: Accept-Encoding
Vary: Origin
Via: 2.0 heroku-router
X-Request-Id: e5ae0c33-b1ac-7e88-1010-f622c950fed5
Content-Length: 68

[{"data":{"searchQuery":{"atsJobs":[],"__typename":"SearchQuery"}}}]
```

Common mechanisms to reduce automated abuse include IP-based rate limiting and CAPTCHAs. However, these mechanisms are not generally sufficient on their own to mitigate the risk of abuse by even moderately sophisticated attackers; instead, most applications need to monitor and quickly react to signals of automated abuse by implementing targeted protections.

Recommendation

A typical security assessment lacks sufficient context to provide useful recommendations on what anti-abuse measures will be useful for a given application. It is recommended that the use of the following measures should be evaluated in terms of the contribution they could make to a strong abuse protection system within this environment:

- Implement proactive monitoring and detection of automated abuse signals to enable fast reaction for abuse of targeted functionality
- Engage and enable members of engineering, customer support, IT, and security teams to share responsibility in managing abusive actors (for example, by creating a system to block abusive accounts or IP addresses)
- For specific, targeted functionality such as unauthenticated forms or public APIs, implement CAPTCHAs or IP-based rate limiting to reduce and discourage attacks

Reproduction Steps

1. Configure a proxy in a Firefox browser and run Burp Suite. Make sure intercept is off by clicking “Proxy” -> “Intercept -> “Intercept is off” in Burp Suite.
2. Prepare intercepting web service request by clicking “Proxy” -> “Intercept” -> “Intercept is on” in Burp Suite.
3. Initiate an HTTP request for the `/api/graphql` history endpoint.
4. In Burp Suite, observe that the request was intercepted in the “Proxy” -> “Intercept” tab.
5. Send the request to the Burp Intruder
6. Use the sniper attack with the null payload that set to 1000 then initiate the attack
7. Observed that the all the request has been successfully completed.

Location

- https://www.gem.com/api/graphql

Info

Insecure Entropy Identifier

Overall Risk	Informational	**Finding ID**	NCC-E030222-7EA
Impact	Low	**Component**	Gem Web Application and Browser Extension Security Assessment
Exploitability	Low	**Category**	Uncategorized
		Status	Reported

Impact

A user with limited role could decode the prospect and candidate IDs, potentially leading to enumeration of all accessible prospect and candidate data.

Description

The Gem web application made use of direct object references using incremental IDs that were encoded in base64 for created prospect users or candidates. As a result, it was possible to enumerate and access user information by decoding the base64 person ID incrementally or decrementally. This was reported in a previous test with NCC and has been reported for informational purposes only as this is an intended functionality. There is also an option to search for available candidates and access their information if it is publicly available within the application.

As shown in the code block and image below, the consultant was able to enumerate a prospect user that was available and created within the gem application.

```
Base64 value : https://www.gem.com/candidate/UGVyc29uOjIyNDk5MDQ5Mg==

Decoded value : Person:224990492
```

Below is a screenshot from the candidate page:

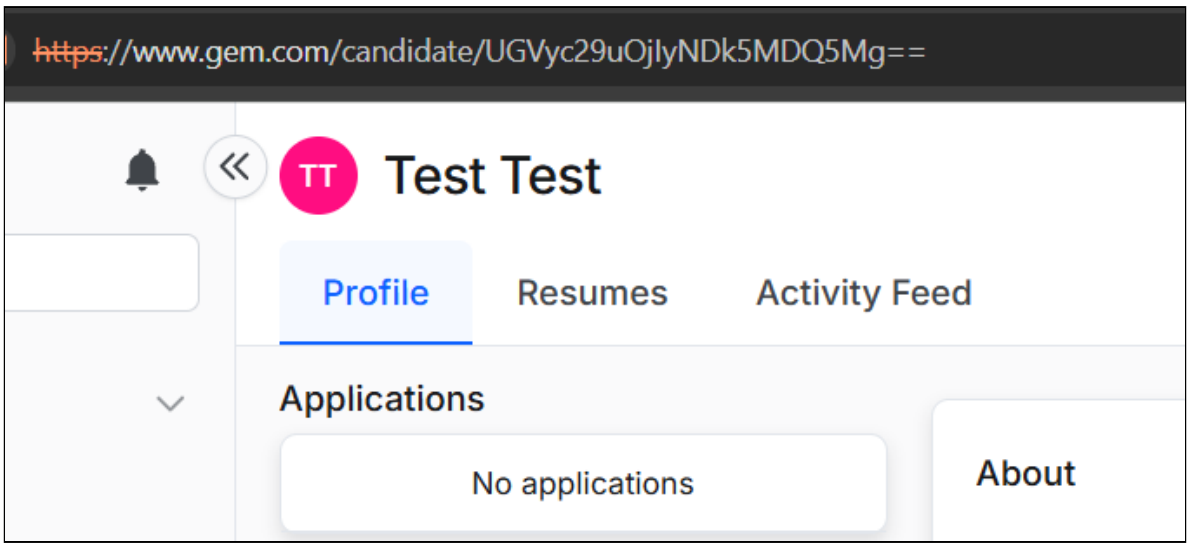

Figure 4: Base64 PersonID in the URL

Recommendation

It is recommended to use a universally unique identifier (UUID) to represent object IDs, rather than incremental integers encoded in base64. This will significantly increase the difficulty for attackers attempting to enumerate public candidate information. The OWASP guidelines suggest the use of the intermediate mapping table model. Dynamically-generated identifiers, rather than incremental integers, should be used to reference existing objects through a mapping table that is associated to the user session or user account.

Reproduction Steps

1. Create a prospect using the admin account.
2. Login as a limited user, then access the prospect ID via the URL with the encoded base64 person ID.
3. Observe that a limited user will be able to access the prospect user and information if it is publicly available.

```
https://www.gem.com/candidate/Person:ID encoded in base64
```

Location

- https://www.gem.com/candidate/`<person:ID>`

5 Finding Field Definitions

The following sections describe the risk rating and category assigned to issues NCC Group identified.

Risk Scale

NCC Group uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors. The risk rating is NCC Group's recommended prioritization for addressing findings. Every organization has a different risk sensitivity, so to some extent these recommendations are more relative than absolute guidelines.

Overall Risk

Overall risk reflects NCC Group's estimation of the risk that a finding poses to the target system or systems. It takes into account the impact of the finding, the difficulty of exploitation, and any other relevant factors.

Rating	Description
Critical	Implies an immediate, easily accessible threat of total compromise.
High	Implies an immediate threat of system compromise, or an easily accessible threat of large-scale breach.
Medium	A difficult to exploit threat of large-scale breach, or easy compromise of a small portion of the application.
Low	Implies a relatively minor threat to the application.
Informational	No immediate threat to the application. May provide suggestions for application improvement, functional issues with the application, or conditions that could later lead to an exploitable finding.

Impact

Impact reflects the effects that successful exploitation has upon the target system or systems. It takes into account potential losses of confidentiality, integrity and availability, as well as potential reputational losses.

Rating	Description
High	Attackers can read or modify all data in a system, execute arbitrary code on the system, or escalate their privileges to superuser level.
Medium	Attackers can read or modify some unauthorized data on a system, deny access to that system, or gain significant internal technical information.
Low	Attackers can gain small amounts of unauthorized information or slightly degrade system performance. May have a negative public perception of security.

Exploitability

Exploitability reflects the ease with which attackers may exploit a finding. It takes into account the level of access required, availability of exploitation information, requirements relating to social engineering, race conditions, brute forcing, etc, and other impediments to exploitation.

Rating	Description
High	Attackers can unilaterally exploit the finding without special permissions or significant roadblocks.

Rating	Description
Medium	Attackers would need to leverage a third party, gain non-public information, exploit a race condition, already have privileged access, or otherwise overcome moderate hurdles in order to exploit the finding.
Low	Exploitation requires implausible social engineering, a difficult race condition, guessing difficult-to-guess data, or is otherwise unlikely.

Category

NCC Group categorizes findings based on the security area to which those findings belong. This can help organizations identify gaps in secure development, deployment, patching, etc.

Category Name	Description
Access Controls	Related to authorization of users, and assessment of rights.
Auditing and Logging	Related to auditing of actions, or logging of problems.
Authentication	Related to the identification of users.
Configuration	Related to security configurations of servers, devices, or software.
Cryptography	Related to mathematical protections for data.
Data Exposure	Related to unintended exposure of sensitive information.
Data Validation	Related to improper reliance on the structure or values of data.
Denial of Service	Related to causing system failure.
Error Reporting	Related to the reporting of error conditions in a secure fashion.
Patching	Related to keeping software up to date.
Session Management	Related to the identification of authenticated users.
Timing	Related to race conditions, locking, or order of operations.

6 Contact Info

The team from NCC Group has the following primary members:

- Matt Weber – Account Manager
  matt.weber@nccgroup.com
- Annie Pearson – Project Manager
  annie.pearson@nccgroup.com
- Carl Jason Mangio – Consultant
  carljason.mangio@nccgroup.com
- Samuel Gabrielle Malijan – Consultant
  samuel.gabriellemalijan@nccgroup.com

The team from Gem has the following primary members:

- Yi-An Lai
  yian@gem.com
- David Dold
  dold@gem.com