F E D E R A C Y

Penetration Test

REPORT
April 02, 2021

Prepared for
Spacelift

Prepared by
James Sulinski
Co-founder & CEO, Federacy

Executive Summary

Spacelift engaged Federacy to perform a penetration test and vulnerability assessment. The objective of the penetration test was to verify that Spacelift's application and its supporting infrastructure are adequately protected with appropriate controls, based on industry standards and best practices. Vulnerabilities, flaws, and defects in the design or implementation of the application, system, and network were sought.

The following categories were covered:

* Authentication
* Session Management
* Access Control
* Validation, Serialization, and Encoding
* Data Protection
* Communication Security
* Application Integrity
* Business Logic
* File and Resource Handling
* API Security
* Configuration and Dependency Security

The target of the penetration test covered app.spacelift.dev. Two security researchers conducted this penetration test between February 26, 2021 and April 01, 2021. Where testing was performed against a staging environment it was confirmed to be an environment that mirrored production, including code and infrastructure.

All significant vulnerabilities discovered were remediated by Spacelift, which was verified by Federacy.

Methodology

Federacy penetration tests are performed using a phased methodology: planning & reconnaissance phase, research phase, and documentation phase.

Planning & Reconnaissance Phase

The planning phase involved information gathering from Spacelift and the formation of Federacy Research and Review teams.

GOALS & OBJECTIVES

The primary goals of the Federacy penetration test were to identify vulnerabilities and validate their remediation in order to comply with regulatory and/or vendor relationship requirements.

SCOPE

Spacelift provided documentation, particularly related to mitigating controls, and a list of assets, including URLs and IPs, to be tested.

Spacelift also provided information regarding network/system architecture as well as segmentation controls and was responsible for ensuring that the established scope encompassed the entirety of the environment's perimeters and all critical systems.

ROLES & RESPONSIBILITIES

The **Federacy Research Team** was selected based on skills exhibited, experience, certifications, and published research.

The **Federacy Review Team**, comprised of members of the Federacy founding team, was responsible for providing remediation guidance to Spacelift as well as validating remediation of vulnerabilities.

The Federacy Research and Review teams were organizationally distinct with no overlap in membership. The Research Team was not involved in remediation or remediation validation of vulnerabilities.

TIMELINE

The penetration test was conducted by the Federacy Research Team within a time period established by Spacelift, taking into account any regulatory and compliance requirements.

ACCESS

Spacelift supplied credentials and/or upgraded accounts when necessary to provide researchers access to test assets. Spacelift produced a list of roles and/or account types and clarified which were in-scope of the penetration test.

INFORMATION GATHERING

Spacelift provided Federacy with details about their stack, infrastructure, and applications, potentially including diagrams and documentation. Spacelift and Federacy discussed scope of the engagement, access levels/roles to be tested, and special areas of interest to Spacelift. These details were augmented through reconnaissance including DNS and directory enumeration, certificate transparency log analysis, OSINT, fingerprinting, port

scanning, and/or other techniques.

Research Phase

During the research phase, the Federacy Research Team evaluated all targets listed as in-scope in order to identify vulnerabilities. Two researchers independently verified all categories of the OWASP Testing Guide Version 5.

TIMELINE

Two security researchers conducted this penetration test between February 26, 2021 and April 01, 2021 for no less than 100 hours of research.

TECHNIQUES

Federacy utilized guidance from the OWASP Testing Guide v5, OWASP Application Security Verification Standard, NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations), NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) and/or ISO 27001. Researchers focused on vulnerabilities impacting authorization, authentication, integrity, confidentiality, and availability.

TOOLING

The Federacy Research Team leveraged open source, proprietary, and/or customized software to facilitate their work; however, the majority of the penetration test involved manual analysis. All automated tools were specifically tailored and configured for Spacelift's applications to minimize impact to systems.

Documentation Phase

REPORTING

The Federacy Research Team submitted all findings to Spacelift's Federacy Inbox, where they were able to be commented upon, assigned, expanded upon, and status tracked. Spacelift was able to review all findings in their Federacy Inbox as well as generate a PDF version of the following reports: penetration test and letter of attestation.

CLASSIFICATION & SEVERITY

The Federacy Research Team classified each finding with an identifier from MITRE's Common Weakness Enumeration (CWE) system. The Research Team also assigned a severity based on the following rubric: Low (configuration issues and limited impact), Medium (limited access to other user's private data), High (full access to other user's private data), Critical (systemic compromise). In each case, the researcher responsible bases these classifications on their professional judgment, past experience, and knowledge of the system being researched.

The Federacy Triage Team may adjust the classification and severity of a finding based on their own professional judgment and experience, with approval from Spacelift.

VALIDATION & REMEDIATION

The Federacy Review Team triaged and validated all findings and offered remediation advice for all valid vulnerabilities. They also analyzed vulnerabilities to look for root causes and commonality in order to provide a more thorough report and corrected or added CWE (Common Weakness Enumeration) tags, severity,

references, PoCs, and remediation advice. When necessary, they communicated with the Federacy Research Team to facilitate this work.

RETESTING

Spacelift was responsible for notifying Federacy of vulnerability remediation, whereupon the Federacy Review Team was then responsible for retesting remediated vulnerabilities to validate successful remediation. The Federacy Research Team played no role in validating the remediation of vulnerabilities.

F E D E R A C Y

PENETRATION TEST REPORT FOR

Spacelift

April 02, 2021

Summary

Status

All significant vulnerabilities remediated

Results

0 Critical
0 High
0 Medium

Scopes

app.spacelift.dev

Researcher Attestations

Artur Czyz, OSCP
@s3curity
April 01, 2021
07:31pm UTC

Gokberk Gulgun, OSCE, OSWE
@tvmsec
April 01, 2021
07:32pm UTC

Findings

ID: 8a4e95

SUMMARY

Lack of X-Content-Type-Options header

SEVERITY

Low

STATUS

Open

DESCRIPTION

The X-Content-Type-Options header is used to mitigate MIME-type sniffing-related attacks, which could be used to bypass a CSP for an XSS attack.

It seems that the GraphQL routes are not returning this header.

IMPACT

Limited potential to bypass CSP.

REMEDIATION ADVICE

Add `X-Content-Type` header

REQUEST

```
POST /graphql HTTP/1.1
Host: jsresearch.app.spacelift.dev
Connection: close
Content-Length: 318
Pragma: no-cache
Cache-Control: no-cache
sec-ch-ua: "Chromium";v="89", ";Not A Brand";v="99"
accept: */*
authorization: Bearer <snip>
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/89.0.4389.90 Safari/537.36
content-type: application/json
Origin: https://jsresearch.app.spacelift.dev
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://jsresearch.app.spacelift.dev/
```

Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: _ga=GA1.2.1716029431.1617239265; _gid=GA1.2.355470232.1617239265; __stripe_mid=dd897c4d-5b59-435d-9ce9-8db2eb5d18877d9d1f; __stripe_sid=e9b889c2-3d37-4642-9e58-ea34f95cf81a62e49b

{"operationName":"GetAccount","variables":{},"query":"query GetAccount {\n ...accountDataFragment\n}\n\nfragment accountDataFragment on Query {\n accountName: name\n accountType: type\n installationId\n viewer {\n id\n admin\n avatarURL\n name\n validUntil\n __typename\n }\n __typename\n}\n"}

RESPONSE

HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 280
Connection: close
Date: Thu, 01 Apr 2021 01:08:59 GMT
Content-Security-Policy: default-src 'none'; script-src 'sha256-jKCDzXEDw0s9EnOZ+WkqfLRDmXB9mVa/hRBqIgIfmLM=';
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
X-Cache: Miss from cloudfront
Via: 1.1 98aedae6661e3904540676966998ed89.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: SEA19-C2
X-Amz-Cf-Id: 9UkhPpBT3Yfm-hJ92iNNoSE0o5-HsYyKbpA4vJjO_QNVi0Ue5PW1rA==

{"data":{"accountName":"jsresearch","accountType":"USER","installationId":"15437564","viewer":{"id":"jsresearch","admin":true,"avatarURL":"https://avatars.githubusercontent.com/u/50061878?v=4","name":"jsresearch","validUntil":1617242905,"__typename":"User"},"__typename":"Query"}}

VULNERABLE URLS

jsresearch.app.spacelift.dev/graphql

REFERENCES

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

SUMMARY

CSP and security headers differ by path

SEVERITY

Low

STATUS

Open

DESCRIPTION

When initially navigating to the Spacelift dashboard at, for example, https://jsresearch.app.spacelift.dev/, a very tight CSP is returned via headers and the X-Content-Types-Options header is set as well:

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 3412
Connection: close
x-amz-id-2: OrVF/R9TTJ7fMOmZUYhj8VO8I8Bl45MiqqsrCOPwh8hYykqepJAI3fU5Rhxtn42fpcjs53kRoK8=
x-amz-request-id: BD5CSMTWXRKFQXTV
Last-Modified: Tue, 30 Mar 2021 16:35:50 GMT
Accept-Ranges: bytes
Server: AmazonS3
Date: Thu, 01 Apr 2021 01:07:43 GMT
ETag: "f72f241923581423d6d7bdc47c6aaa8c"
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
Referrer-Policy: same-origin
Content-Security-Policy: report-uri https://spacelift.uriports.com/reports/report; report-to default; frame-ancestors 'self'
[...]

However, after logging in, if a user navigates directly to a page, for example, https://jsresearch.app.spacelift.dev/stack/test2, a much looser CSP is returned via meta tags and the X-Content-Types-Options header is missing:

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 3412
Connection: close
Last-Modified: Tue, 30 Mar 2021 16:35:50 GMT

Accept-Ranges: bytes
Server: AmazonS3
Date: Thu, 01 Apr 2021 01:08:23 GMT
ETag: "f72f241923581423d6d7bdc47c6aaa8c"
X-Cache: Error from cloudfront
Via: 1.1 5565a51537c689d1d16f6b4d41f40082.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: SEA19-C2
X-Amz-Cf-Id: 24plDzPWUZKZ0pEHXVHsqNqNKuMDnoJdQPKxQ-YZW9gfbbz1u012Yw==
Age: 1310

[...]

<meta http-equiv="Content-Security-Policy" content="base-uri 'self'; object-src 'none'; script-src 'self' https://www.google-analytics.com https://www.googletagmanager.com https://www.googleadservices.com https://googleads.g.doubleclick.net https://www.google.com https://js.stripe.com https://js.hscollectedforms.net https://js.usemessages.com https://js.hs-banner.com https://js.hs-analytics.net https://js.hsadspixel.net https://forms.hsforms.com https://static.hsappstatic.net cdn.mouseflow.com https://o2.mouseflow.com js.hs-scripts.com https://connect.facebook.net https://hubspot-forms-static-embed.s3.amazonaws.com 'nonce-1RSHDpRfjSvEwuEzwCcF3A==' 'nonce-LDNNFOhPThC5YaQZjkc5dA==' 'nonce-VhRQvE8rq4DhOP/YddzDvw==' 'nonce-z4R67bgDAEV+5vEcJQetvw==' 'nonce-JIbARFQiJCHmJH2pIncyFA==''; style-src 'self' 'unsafe-inline'; default-src 'none'; img-src 'self' https:; font-src 'self'; form-action 'self'; manifest-src 'self'; frame-src 'self' https://js.stripe.com https://r5ljfdhtqdl1.statuspage.io https://app.hubspot.com https://meetings.hubspot.com https://www.google.com/ https://forms.hsforms.com/; connect-src 'self' https://sessions.bugsnag.com https://notify.bugsnag.com https://js.stripe.com https://www.google-analytics.com https://api.hubspot.com https://track.hubspot.com https://forms.hubspot.com https://api.hubapi.com https://stats.g.doubleclick.net https://static.hsappstatic.net https://o2.mouseflow.com https://forms.hsforms.com https://spacelift-uploads20200730121739867600000000c.s3.eu-west-1.amazonaws.com">

IMPACT

Potential to run unauthorized code/XSS.

REMEDIATION ADVICE

Add X-Content-Type-Options header and make CSP consistent, ideally utilizing headers rather than meta tags.

VULNERABLE URLS

https://jsresearch.app.spacelift.dev/stack/test2

REFERENCES

https://developers.google.com/web/fundamentals/security/csp

SUMMARY

Sensitive information stored in localStorage (token)

SEVERITY

Low

STATUS

Open

DESCRIPTION

The auth token is stored in localStorage. This can be problematic because localStorage is vulnerable to being accessed by Javascript, which means the tokens could be exfiltrated. httpOnly cookies do not have this problem, but can also be abused via XSS in a more limited fashion.

It should be noted that this is a disputed best practice. While NIST 800-63B, the OWASP Cheat Sheets, OWASP Testing Guide, Bugcrowd Vulnerability Rating Taxonomy, and many others consider it inappropriate to store sensitive tokens in localStorage, the OWASP ASVS and other community members consider it acceptable.

IMPACT

Potential for account compromise

REMEDIATION ADVICE

Consider utilizing httpOnly cookies with other security attributes set. This will also require implementing CSRF mitigations.

REFERENCES

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#security-risks

https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html#storage-apis

https://www.rdegges.com/2018/please-stop-using-local-storage/

SUMMARY

Insufficient cache controls

SEVERITY

Low

STATUS

Open

DESCRIPTION

Lack of `cache-control`, `last-modified`, `expires` and `pragma` headers could lead to sensitive data being cached, including in intermediary devices like proxies.

IMPACT

Potential for sensitive information disclosure

CWES

CWE-525: Cache Control For A Sensitive Page

REMEDIATION ADVICE

Implement `cache-control`, `last-modified`, `expires` and `pragma` headers where relevant and missing.

RESPONSE

HTTP/1.1 200 OK
Content-Type: application/json
Connection: close
Date: Thu, 01 Apr 2021 04:52:45 GMT
Content-Security-Policy: default-src 'none'; script-src 'sha256-jKCDzXEDw0s9EnOZ+WkqfLRDmXB9mVa/hRBqIgIfmLM=';
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
X-Cache: Miss from cloudfront
Via: 1.1 4f3feb5c4393987d42d1971d404d7cea.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: SEA19-C2
X-Amz-Cf-Id: ZjS7ABixTNB22amUOywkufACKtEFl2Dd6F6-osAdGkL_JmF1NSOzow==
Content-Length: 3600

REFERENCES

https://github.com/OWASP/ASVS/blob/master/4.0/en/0x16-V8-Data-Protection.md#v81-general-data-protection

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

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

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

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

SUMMARY

Lack of session invalidation on logout

SEVERITY

Low

STATUS

Open

DESCRIPTION

The session isn't invalidated when a user logs out. Further, the session token that's stored in localStorage is not cleared.

Session termination is an important part of the session lifecycle. Reducing to a minimum the lifetime of the session tokens decreases the likelihood of a successful session hijacking attack.

Enabling users to log out and clear localStorage is also important for shared computers.

Proof of Concept

1. Browse to https://[username].app.spacelift.dev/.
2. Proxy traffic with Burp or open developer console and monitor network tab
3. Log in
4. Once logged in, log out
5. Replay a previous request

IMPACT

Potential for account compromise and session replay attacks.

CWES

CWE-613: Failure To Invalidate Session

REMEDIATION ADVICE

Invalidate the session on the server-side on log out.
Clear localStorage.

VULNERABLE URLS

https://username.app.spacelift.dev/

REFERENCES

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#session-expiration

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/06-Session_Management_Testing/06-Testing_for_Logout_Functionality

Disclaimer

No trademark, copyright, or patent licenses are expressly or implicitly granted with this analysis, report, or white paper. All brand names and product names used in this document are trademarks, registered trademarks, or trade names of their respective holders. Federacy Cypher, Inc is not associated with any vendors or products mentioned in this document.

A penetration test is a snapshot in time. The findings and recommendations reflect the information gathered during the penetration test and not any changes or modifications made outside of that period. Engagements with time limitations do not always allow for a full evaluation of all security controls. Federacy prioritized identifying the weakest security controls an attacker could exploit. Federacy recommends conducting similar penetration tests as regularly as possible, at least anually.

Confidentiality Notice

This document contains information confidential and proprietary to Federacy Cypher, Inc and the company identified as Spacelift. The information may not be used, disclosed, or reproduced without the prior written consent of Federacy Cypher, Inc.