# BEAPENGINE Vulnerability Report 1

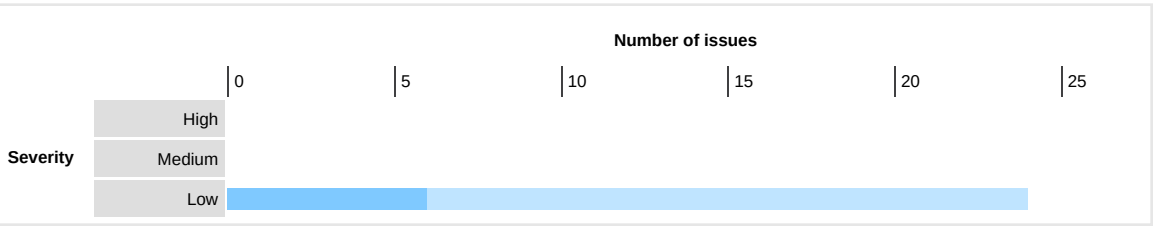
Burp Suite Professional

## Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low, Information or False Positive. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

| | | Confidence | | | |
|---|---|---|---|---|---|
| | | Certain | Firm | Tentative | Total |
| Severity | High | 0 | 0 | 0 | 0 |
| | Medium | 0 | 0 | 0 | 0 |
| | Low | 0 | 6 | 18 | 24 |
| | Information | 19 | 2 | 0 | 21 |
| | False Positive | 0 | 0 | 0 | 0 |

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.




## Contents

# 1. Client-side JSON injection (DOM-based)

There are 6 instances of this issue:

- /
- /
- /about-us
- /about-us
- /privacy-policy
- /privacy-policy

## Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based JSON injection arises when a script incorporates controllable data into a string that is parsed as a JSON data structure and then processed by the application. An attacker may be able to use this behavior to construct a URL that, if visited by another application user, will cause arbitrary JSON data to be processed. Depending on the purpose for which this data is used, it may be possible to subvert the application's logic, or cause unintended actions on behalf of the user.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

## Issue remediation

The most effective way to avoid DOM-based JSON injection vulnerabilities is not to parse as JSON any string containing data that originated from an untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from modifying the JSON structure in inappropriate ways. This may involve strict validation of specific items to ensure they do not contain any characters that may interfere with the structure of the JSON when it is parsed.

## References

- Web Security Academy: Client-side JSON injection (DOM-based)

## Vulnerability classifications

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CWE-116: Improper Encoding or Escaping of Output
- CWE-159: Failure to Sanitize Special Element
- CAPEC-153: Input Data Manipulation

## 1.1. http://localhost:3000/

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Firm** |
| Host: | **http://localhost:3000** |
| Path: | **/** |

### Issue detail

The application may be vulnerable to DOM-based client-side JSON injection. Data is read from **document.cookie** and passed to **JSON.parse**.

Because the data originates from a cookie, the application's behavior is not trivial to exploit in an attack against another user. Typically, you will need to find a means of setting an arbitrary cookie value in the victim's browser in order to exploit the vulnerability. Applications often contain "cookie-forcing" conditions which make this possible, and such a condition in any related domain or subdomain can potentially be used for this purpose. Nonetheless, this limitation somewhat mitigates the impact of the vulnerability.

## Request

```
GET / HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:34:01 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

## Dynamic analysis

Data is read from **document.cookie** and passed to **JSON.parse**.

The previous value reached the sink as:

```
ksc6c0x5st%27%22`'"/ksc6c0x5st/><ksc6c0x5st/\>iq7qrado3t&
```

The stack trace at the source was:

```
at Object.<computed>.get (<anonymous>:1:624755)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99247:73)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.iPcCb (<anonymous>:1:505498)
at _0x464a84.PcEKj._0x2950e0.<computed> (<anonymous>:1:528870)
at readCookie (http://localhost:3000/static/js/bundle.js:99222:19)
at http://localhost:3000/static/js/bundle.js:99266:18
at Set.forEach (<anonymous>)
at Cookies._checkChanges (http://localhost:3000/static/js/bundle.js:99262:11)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99248:12)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
```

```
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

This was triggered by a **message** event.

---

## 1.2. http://localhost:3000/

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Firm** |
| Host: | **http://localhost:3000** |
| Path: | **/** |

### Issue detail

The application may be vulnerable to DOM-based client-side JSON injection. Data is read from **document.cookie** and passed to **JSON.parse**.

Because the data originates from a cookie, the application's behavior is not trivial to exploit in an attack against another user. Typically, you will need to find a means of setting an arbitrary cookie value in the victim's browser in order to exploit the vulnerability. Applications often contain "cookie-forcing" conditions which make this possible, and such a condition in any related domain or subdomain can potentially be used for this purpose. Nonetheless, this limitation somewhat mitigates the impact of the vulnerability.

### Request

```
GET / HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:34:01 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

### Dynamic analysis

Data is read from **document.cookie** and passed to **JSON.parse**.

The previous value reached the sink as:

```
j9599l6vlf%27%22`'"/j9599l6vlf/><j9599l6vlf/\>q0va4wkg4t&
```

The stack trace at the source was:

```
at Object.<computed>.get (<anonymous>:1:624755)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99247:73)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
```

```
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

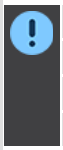
```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.iPcCb (<anonymous>:1:505498)
at _0x464a84.PcEKj._0x2950e0.<computed> (<anonymous>:1:528870)
at readCookie (http://localhost:3000/static/js/bundle.js:99222:19)
at http://localhost:3000/static/js/bundle.js:99266:18
at Set.forEach (<anonymous>)
at Cookies._checkChanges (http://localhost:3000/static/js/bundle.js:99262:11)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99248:12)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

This was triggered by a **message** event.

---

## 1.3. http://localhost:3000/about-us

### Summary



| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Firm** |
| Host: | **http://localhost:3000** |
| Path: | **/about-us** |

### Issue detail

The application may be vulnerable to DOM-based client-side JSON injection. Data is read from **document.cookie** and passed to **JSON.parse**.

Because the data originates from a cookie, the application's behavior is not trivial to exploit in an attack against another user. Typically, you will need to find a means of setting an arbitrary cookie value in the victim's browser in order to exploit the vulnerability. Applications often contain "cookie-forcing" conditions which make this possible, and such a condition in any related domain or subdomain can potentially be used for this purpose. Nonetheless, this limitation somewhat mitigates the impact of the vulnerability.

### Request

```
GET /about-us HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
```

```
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:28 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

## Dynamic analysis

Data is read from **document.cookie** and passed to **JSON.parse**.

The previous value reached the sink as:

```
l097y0ybly%27%22`'"/l097y0ybly/><l097y0ybly/\>ditno96g34&
```

The stack trace at the source was:

```
at Object.<computed>.get (<anonymous>:1:624755)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99247:73)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.iPcCb (<anonymous>:1:505498)
at _0x464a84.PcEKj._0x2950e0.<computed> (<anonymous>:1:528870)
at readCookie (http://localhost:3000/static/js/bundle.js:99222:19)
at http://localhost:3000/static/js/bundle.js:99266:18
at Set.forEach (<anonymous>)
at Cookies._checkChanges (http://localhost:3000/static/js/bundle.js:99262:11)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99248:12)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

This was triggered by a **message** event.

---

## 1.4. http://localhost:3000/about-us

## Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Firm** |
| Host: | **http://localhost:3000** |
| Path: | **/about-us** |

## Issue detail

The application may be vulnerable to DOM-based client-side JSON injection. Data is read from **document.cookie** and passed to **JSON.parse**.

Because the data originates from a cookie, the application's behavior is not trivial to exploit in an attack against another user. Typically, you will need to find a means of setting an arbitrary cookie value in the victim's browser in order to exploit the vulnerability. Applications often contain "cookie-forcing" conditions which make this possible, and such a condition in any related domain or subdomain can potentially be used for this purpose. Nonetheless, this limitation somewhat mitigates the impact of the vulnerability.

## Request

```
GET /about-us HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:28 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

## Dynamic analysis

Data is read from **document.cookie** and passed to **JSON.parse**.

The previous value reached the sink as:

```
twckyysyeu%27%22`'"/twckyysyeu/><twckyysyeu/\>lvs5dq8oru&
```

The stack trace at the source was:

```
at Object.<computed>.get (<anonymous>:1:624755)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99247:73)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.iPcCb (<anonymous>:1:505498)
at _0x464a84.PcEKj._0x2950e0.<computed> (<anonymous>:1:528870)
at readCookie (http://localhost:3000/static/js/bundle.js:99222:19)
at http://localhost:3000/static/js/bundle.js:99266:18
at Set.forEach (<anonymous>)
at Cookies._checkChanges (http://localhost:3000/static/js/bundle.js:99262:11)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99248:12)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
```

```
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

This was triggered by a **message** event.

---

## 1.5. http://localhost:3000/privacy-policy

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Firm** |
| Host: | **http://localhost:3000** |
| Path: | **/privacy-policy** |

### Issue detail

The application may be vulnerable to DOM-based client-side JSON injection. Data is read from **document.cookie** and passed to **JSON.parse**.

Because the data originates from a cookie, the application's behavior is not trivial to exploit in an attack against another user. Typically, you will need to find a means of setting an arbitrary cookie value in the victim's browser in order to exploit the vulnerability. Applications often contain "cookie-forcing" conditions which make this possible, and such a condition in any related domain or subdomain can potentially be used for this purpose. Nonetheless, this limitation somewhat mitigates the impact of the vulnerability.

### Request

```
GET /privacy-policy HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:24 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

### Dynamic analysis

Data is read from **document.cookie** and passed to **JSON.parse**.

The previous value reached the sink as:

```
gimfm1ivz1%27%22`'"/gimfm1ivz1/><gimfm1ivz1/\>lzrt8i7fs2&
```

The stack trace at the source was:

```
at Object.<computed>.get (<anonymous>:1:624755)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99247:73)
```

```
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

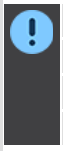
```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.iPcCb (<anonymous>:1:505498)
at _0x464a84.PcEKj._0x2950e0.<computed> (<anonymous>:1:528870)
at readCookie (http://localhost:3000/static/js/bundle.js:99222:19)
at http://localhost:3000/static/js/bundle.js:99266:18
at Set.forEach (<anonymous>)
at Cookies._checkChanges (http://localhost:3000/static/js/bundle.js:99262:11)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99248:12)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

This was triggered by a **message** event.

---

## 1.6. http://localhost:3000/privacy-policy

### Summary



| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Firm** |
| Host: | **http://localhost:3000** |
| Path: | **/privacy-policy** |

### Issue detail

The application may be vulnerable to DOM-based client-side JSON injection. Data is read from **document.cookie** and passed to **JSON.parse**.

Because the data originates from a cookie, the application's behavior is not trivial to exploit in an attack against another user. Typically, you will need to find a means of setting an arbitrary cookie value in the victim's browser in order to exploit the vulnerability. Applications often contain "cookie-forcing" conditions which make this possible, and such a condition in any related domain or subdomain can potentially be used for this purpose. Nonetheless, this limitation somewhat mitigates the impact of the vulnerability.

### Request

```
GET /privacy-policy HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:24 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

### Dynamic analysis

Data is read from **document.cookie** and passed to **JSON.parse**.

The previous value reached the sink as:

```
kd9c6j11r1%27%22`'"/kd9c6j11r1/><kd9c6j11r1/\>l9ugl7chp0&
```

The stack trace at the source was:

```
at Object.<computed>.get (<anonymous>:1:624755)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99247:73)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.iPcCb (<anonymous>:1:505498)
at _0x464a84.PcEKj._0x2950e0.<computed> (<anonymous>:1:528870)
at readCookie (http://localhost:3000/static/js/bundle.js:99222:19)
at http://localhost:3000/static/js/bundle.js:99266:18
at Set.forEach (<anonymous>)
at Cookies._checkChanges (http://localhost:3000/static/js/bundle.js:99262:11)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99248:12)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

This was triggered by a **message** event.

## 2. Open redirection (DOM-based)

There are 18 instances of this issue:

- /
- /
- /
- /
- /
- /
- /about-us
- /about-us
- /about-us
- /about-us
- /about-us
- /about-us
- /privacy-policy
- /privacy-policy
- /privacy-policy
- /privacy-policy
- /privacy-policy
- /privacy-policy

## Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based open redirection arises when a script writes controllable data into the target of a redirection in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

**Note:** If an attacker is able to control the start of the string that is passed to the redirection API, then it may be possible to escalate this vulnerability into a JavaScript injection attack, by using a URL with the javascript: pseudo-protocol to execute arbitrary script code when the URL is processed by the browser.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

## Issue remediation

The most effective way to avoid DOM-based open redirection vulnerabilities is not to dynamically set redirection targets using data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing an arbitrary URL as a redirection target. In general, this is best achieved by using a whitelist of URLs that are permitted redirection targets, and strictly validating the target against this list before performing the redirection.

## References

- Web Security Academy: Open redirection (DOM-based)

## Vulnerability classifications

- CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

---

# 2.1. http://localhost:3000/

## Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/** |

## Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.search** and passed to **xhr.send**.

## Request

```
GET / HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:34:01 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

## Dynamic analysis

Data is read from **location.search** and passed to **xhr.send**.

The following value was injected into the source:

```
?o5q32l299m=o5q32l299m%27%22`'"/o5q32l299m/><o5q32l299m/\>mtwqx04mki&
```

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get search (<anonymous>:1:323065)
at Array.<anonymous> (http://localhost:3000/static/js/bundle.js:83675:84)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.addBaseInfo (http://localhost:3000/static/js/bundle.js:83670:13)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.ensureItemHasSomethingToSay (http://localhost:3000/static/js/bundle.js:83652:111)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleItemWithError (http://localhost:3000/static/js/bundle.js:83649:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleDomException (http://localhost:3000/static/js/bundle.js:83629:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at o._applyTransforms (http://localhost:3000/static/js/bundle.js:83257:7)
at o.log (http://localhost:3000/static/js/bundle.js:83245:12)
at a._log (http://localhost:3000/static/js/bundle.js:83025:202)
at a.info (http://localhost:3000/static/js/bundle.js:82996:12)
at m.info (http://localhost:3000/static/js/bundle.js:82805:26)
at Navbar (http://localhost:3000/static/js/bundle.js:1048:11)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

---

## 2.2. http://localhost:3000/

## Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/** |

## Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.href** and passed to **xhr.send**.

## Request

```
GET / HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:34:01 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

## Dynamic analysis

Data is read from **location.href** and passed to **xhr.send**.

The following value was injected into the source:

```
http://localhost:3000/?gmitogj7fx=gmitogj7fx%27%22`'"/gmitogj7fx/><gmitogj7fx/\>h7muned2kp&#gmitogj7fx=gmitogj7fx%27%22`'"/gmitogj7fx/><gmito
```

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href (<anonymous>:1:323401)
at Array.<anonymous> (http://localhost:3000/static/js/bundle.js:83675:50)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.addBaseInfo (http://localhost:3000/static/js/bundle.js:83670:13)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.ensureItemHasSomethingToSay (http://localhost:3000/static/js/bundle.js:83652:111)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleItemWithError (http://localhost:3000/static/js/bundle.js:83649:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleDomException (http://localhost:3000/static/js/bundle.js:83629:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at o._applyTransforms (http://localhost:3000/static/js/bundle.js:83257:7)
at o.log (http://localhost:3000/static/js/bundle.js:83245:12)
at a._log (http://localhost:3000/static/js/bundle.js:83025:202)
at a.info (http://localhost:3000/static/js/bundle.js:82996:12)
at m.info (http://localhost:3000/static/js/bundle.js:82805:26)
at Navbar (http://localhost:3000/static/js/bundle.js:1048:11)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
```

```
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

---

## 2.3. http://localhost:3000/

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/** |

### Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.search** and passed to **xhr.send**.

### Request

```
GET / HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:34:01 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

### Dynamic analysis

Data is read from **location.search** and passed to **xhr.send**.

The following value was injected into the source:

```
?lihqtnbq00=lihqtnbq00%27%22`'"/lihqtnbq00/><lihqtnbq00/\>y9cv7s9ruk&
```

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get search (<anonymous>:1:323065)
at Array.<anonymous> (http://localhost:3000/static/js/bundle.js:83675:84)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.addBaseInfo (http://localhost:3000/static/js/bundle.js:83670:13)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.ensureItemHasSomethingToSay (http://localhost:3000/static/js/bundle.js:83652:111)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleItemWithError (http://localhost:3000/static/js/bundle.js:83649:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleDomException (http://localhost:3000/static/js/bundle.js:83629:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at o._applyTransforms (http://localhost:3000/static/js/bundle.js:83257:7)
```

```
at o.log (http://localhost:3000/static/js/bundle.js:83245:12)
at a._log (http://localhost:3000/static/js/bundle.js:83025:202)
at a.info (http://localhost:3000/static/js/bundle.js:82996:12)
at m.info (http://localhost:3000/static/js/bundle.js:82805:26)
at Navbar (http://localhost:3000/static/js/bundle.js:1048:11)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

---

## 2.4. http://localhost:3000/

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/** |

### Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.href** and passed to **xhr.send**.

### Request

```
GET / HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:34:01 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

### Dynamic analysis

Data is read from **location.href** and passed to **xhr.send**.

The following value was injected into the source:

```
http://localhost:3000/?h2dcqk4kl3=h2dcqk4kl3%27%22`'"/h2dcqk4kl3/><h2dcqk4kl3/\>bdstum0xzo&#h2dcqk4kl3=h2dcqk4kl3%27%22`'"/h2dcqk4kl3/><h2dcq
```

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href (<anonymous>:1:323401)
at Array.<anonymous> (http://localhost:3000/static/js/bundle.js:83675:50)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.addBaseInfo (http://localhost:3000/static/js/bundle.js:83670:13)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.ensureItemHasSomethingToSay (http://localhost:3000/static/js/bundle.js:83652:111)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleItemWithError (http://localhost:3000/static/js/bundle.js:83649:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleDomException (http://localhost:3000/static/js/bundle.js:83629:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at o._applyTransforms (http://localhost:3000/static/js/bundle.js:83257:7)
at o.log (http://localhost:3000/static/js/bundle.js:83245:12)
at a._log (http://localhost:3000/static/js/bundle.js:83025:202)
at a.info (http://localhost:3000/static/js/bundle.js:82996:12)
at m.info (http://localhost:3000/static/js/bundle.js:82805:26)
at Navbar (http://localhost:3000/static/js/bundle.js:1048:11)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

---

## 2.5. http://localhost:3000/

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/** |

### Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **document.cookie** and passed to **xhr.send**.

Because the data originates from a cookie, the application's behavior is not trivial to exploit in an attack against another user. Typically, you will need to find a means of setting an arbitrary cookie value in the victim's browser in order to exploit the vulnerability. Applications often contain "cookie-forcing" conditions which make this possible, and such a condition in any related domain or subdomain can potentially be used for this purpose. Nonetheless, this limitation somewhat mitigates the impact of the vulnerability.

### Request

```
GET / HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
```

```
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:34:01 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

### Dynamic analysis

Data is read from **document.cookie** and passed to **xhr.send**.

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object.<computed>.get (<anonymous>:1:624755)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99247:73)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

This was triggered by a **message** event.

---

## 2.6. http://localhost:3000/

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/** |

### Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **document.cookie** and passed to **xhr.send**.

Because the data originates from a cookie, the application's behavior is not trivial to exploit in an attack against another user. Typically, you will need to find a means of setting an arbitrary cookie value in the victim's browser in order to exploit the vulnerability. Applications often contain "cookie-forcing" conditions which make this possible, and such a condition in any related domain or subdomain can potentially be used for this purpose. Nonetheless, this limitation somewhat mitigates the impact of the vulnerability.

## Request

```
GET / HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:34:01 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

## Dynamic analysis

Data is read from **document.cookie** and passed to **xhr.send**.

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object.<computed>.get (<anonymous>:1:624755)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99247:73)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

This was triggered by a **message** event.

## 2.7. http://localhost:3000/about-us

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/about-us** |

### Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.search** and passed to **xhr.send**.

### Request

```
GET /about-us HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:28 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

### Dynamic analysis

Data is read from **location.search** and passed to **xhr.send**.

The following value was injected into the source:

```
?nx3u2awbdp=nx3u2awbdp%27%22`'"/nx3u2awbdp/><nx3u2awbdp/\>cwnf9gth2b&
```

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get search (<anonymous>:1:323065)
at Array.<anonymous> (http://localhost:3000/static/js/bundle.js:83675:84)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.addBaseInfo (http://localhost:3000/static/js/bundle.js:83670:13)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.ensureItemHasSomethingToSay (http://localhost:3000/static/js/bundle.js:83652:111)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleItemWithError (http://localhost:3000/static/js/bundle.js:83649:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleDomException (http://localhost:3000/static/js/bundle.js:83629:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at o._applyTransforms (http://localhost:3000/static/js/bundle.js:83257:7)
at o.log (http://localhost:3000/static/js/bundle.js:83245:12)
at a._log (http://localhost:3000/static/js/bundle.js:83025:202)
at a.info (http://localhost:3000/static/js/bundle.js:82996:12)
at m.info (http://localhost:3000/static/js/bundle.js:82805:26)
at Navbar (http://localhost:3000/static/js/bundle.js:1048:11)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
```

```
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

---

## 2.8. http://localhost:3000/about-us

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/about-us** |

### Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.href** and passed to **xhr.send**.

### Request

```
GET /about-us HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:28 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

### Dynamic analysis

Data is read from **location.href** and passed to **xhr.send**.

The following value was injected into the source:

```
http://localhost:3000/about-us?ddz9l39x58=ddz9l39x58%27%22`'"/ddz9l39x58/><ddz9l39x58/\>kbrb1v1yjx&#ddz9l39x58=ddz9l39x58%27%22`'"/ddz9l39x58
```

The previous value reached the sink as:

{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href (<anonymous>:1:323401)
at Array.<anonymous> (http://localhost:3000/static/js/bundle.js:83675:50)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.addBaseInfo (http://localhost:3000/static/js/bundle.js:83670:13)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.ensureItemHasSomethingToSay (http://localhost:3000/static/js/bundle.js:83652:111)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleItemWithError (http://localhost:3000/static/js/bundle.js:83649:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleDomException (http://localhost:3000/static/js/bundle.js:83629:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at o._applyTransforms (http://localhost:3000/static/js/bundle.js:83257:7)
at o.log (http://localhost:3000/static/js/bundle.js:83245:12)
at a._log (http://localhost:3000/static/js/bundle.js:83025:202)
at a.info (http://localhost:3000/static/js/bundle.js:82996:12)
at m.info (http://localhost:3000/static/js/bundle.js:82805:26)
at Navbar (http://localhost:3000/static/js/bundle.js:1048:11)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

---

## 2.9. http://localhost:3000/about-us

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/about-us** |

### Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.search** and passed to **xhr.send**.

### Request

```
GET /about-us HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
```

```
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:28 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

## Dynamic analysis

Data is read from **location.search** and passed to **xhr.send**.

The following value was injected into the source:

```
?aihf0nh3o6=aihf0nh3o6%27%22`'"/aihf0nh3o6/><aihf0nh3o6/\>di5zh52dvv&
```

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get search (<anonymous>:1:323065)
at Array.<anonymous> (http://localhost:3000/static/js/bundle.js:83675:84)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.addBaseInfo (http://localhost:3000/static/js/bundle.js:83670:13)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.ensureItemHasSomethingToSay (http://localhost:3000/static/js/bundle.js:83652:111)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleItemWithError (http://localhost:3000/static/js/bundle.js:83649:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleDomException (http://localhost:3000/static/js/bundle.js:83629:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at o._applyTransforms (http://localhost:3000/static/js/bundle.js:83257:7)
at o.log (http://localhost:3000/static/js/bundle.js:83245:12)
at a._log (http://localhost:3000/static/js/bundle.js:83025:202)
at a.info (http://localhost:3000/static/js/bundle.js:82996:12)
at m.info (http://localhost:3000/static/js/bundle.js:82805:26)
at Navbar (http://localhost:3000/static/js/bundle.js:1048:11)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

---

# 2.10. http://localhost:3000/about-us

## Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/about-us** |

## Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.href** and passed to **xhr.send**.

## Request

```
GET /about-us HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:28 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

## Dynamic analysis

Data is read from **location.href** and passed to **xhr.send**.

The following value was injected into the source:

```
http://localhost:3000/about-us?nfonb5hxm8=nfonb5hxm8%27%22`'"/nfonb5hxm8/><nfonb5hxm8/\>oy4zjniwas&#nfonb5hxm8=nfonb5hxm8%27%22`'"/nfonb5hxm8
```

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href (<anonymous>:1:323401)
at Array.<anonymous> (http://localhost:3000/static/js/bundle.js:83675:50)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.addBaseInfo (http://localhost:3000/static/js/bundle.js:83670:13)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.ensureItemHasSomethingToSay (http://localhost:3000/static/js/bundle.js:83652:111)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleItemWithError (http://localhost:3000/static/js/bundle.js:83649:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleDomException (http://localhost:3000/static/js/bundle.js:83629:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at o._applyTransforms (http://localhost:3000/static/js/bundle.js:83257:7)
at o.log (http://localhost:3000/static/js/bundle.js:83245:12)
at a._log (http://localhost:3000/static/js/bundle.js:83025:202)
at a.info (http://localhost:3000/static/js/bundle.js:82996:12)
at m.info (http://localhost:3000/static/js/bundle.js:82805:26)
at Navbar (http://localhost:3000/static/js/bundle.js:1048:11)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
```

```
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

---

## 2.11. http://localhost:3000/about-us

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/about-us** |

### Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **document.cookie** and passed to **xhr.send**.

Because the data originates from a cookie, the application's behavior is not trivial to exploit in an attack against another user. Typically, you will need to find a means of setting an arbitrary cookie value in the victim's browser in order to exploit the vulnerability. Applications often contain "cookie-forcing" conditions which make this possible, and such a condition in any related domain or subdomain can potentially be used for this purpose. Nonetheless, this limitation somewhat mitigates the impact of the vulnerability.

### Request

```
GET /about-us HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:28 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

### Dynamic analysis

Data is read from **document.cookie** and passed to **xhr.send**.

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object.<computed>.get (<anonymous>:1:624755)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99247:73)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
```

```
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

This was triggered by a **message** event.

---

## 2.12. http://localhost:3000/about-us

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/about-us** |

### Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **document.cookie** and passed to **xhr.send**.

Because the data originates from a cookie, the application's behavior is not trivial to exploit in an attack against another user. Typically, you will need to find a means of setting an arbitrary cookie value in the victim's browser in order to exploit the vulnerability. Applications often contain "cookie-forcing" conditions which make this possible, and such a condition in any related domain or subdomain can potentially be used for this purpose. Nonetheless, this limitation somewhat mitigates the impact of the vulnerability.

### Request

```
GET /about-us HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:28 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

### Dynamic analysis

Data is read from **document.cookie** and passed to **xhr.send**.

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object.<computed>.get (<anonymous>:1:624755)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99247:73)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

This was triggered by a **message** event.

---

## 2.13. http://localhost:3000/privacy-policy

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/privacy-policy** |

### Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.search** and passed to **xhr.send**.

### Request

```
GET /privacy-policy HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:24 GMT
Connection: close
Content-Length: 14009
```

```
<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

## Dynamic analysis

Data is read from **location.search** and passed to **xhr.send**.

The following value was injected into the source:

```
?kqelvcikoz=kqelvcikoz%27%22`'"/kqelvcikoz/><kqelvcikoz/\>e7x12i0tbz&
```

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get search (<anonymous>:1:323065)
at Array.<anonymous> (http://localhost:3000/static/js/bundle.js:83675:84)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.addBaseInfo (http://localhost:3000/static/js/bundle.js:83670:13)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.ensureItemHasSomethingToSay (http://localhost:3000/static/js/bundle.js:83652:111)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleItemWithError (http://localhost:3000/static/js/bundle.js:83649:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleDomException (http://localhost:3000/static/js/bundle.js:83629:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at o._applyTransforms (http://localhost:3000/static/js/bundle.js:83257:7)
at o.log (http://localhost:3000/static/js/bundle.js:83245:12)
at a._log (http://localhost:3000/static/js/bundle.js:83025:202)
at a.info (http://localhost:3000/static/js/bundle.js:82996:12)
at m.info (http://localhost:3000/static/js/bundle.js:82805:26)
at Navbar (http://localhost:3000/static/js/bundle.js:1048:11)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

---

## 2.14. http://localhost:3000/privacy-policy

## Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/privacy-policy** |

## Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.href** and passed to **xhr.send**.

## Request

```
GET /privacy-policy HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
```

```
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:24 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

## Dynamic analysis

Data is read from **location.href** and passed to **xhr.send**.

The following value was injected into the source:

```
http://localhost:3000/privacy-policy?l2frzgnft4=l2frzgnft4%27%22`'"/l2frzgnft4/><l2frzgnft4/\>lqqz6foky5&#l2frzgnft4=l2frzgnft4%27%22`'"/l2fr
```

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href (<anonymous>:1:323401)
at Array.<anonymous> (http://localhost:3000/static/js/bundle.js:83675:50)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.addBaseInfo (http://localhost:3000/static/js/bundle.js:83670:13)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.ensureItemHasSomethingToSay (http://localhost:3000/static/js/bundle.js:83652:111)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleItemWithError (http://localhost:3000/static/js/bundle.js:83649:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleDomException (http://localhost:3000/static/js/bundle.js:83629:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at o._applyTransforms (http://localhost:3000/static/js/bundle.js:83257:7)
at o.log (http://localhost:3000/static/js/bundle.js:83245:12)
at a._log (http://localhost:3000/static/js/bundle.js:83025:202)
at a.info (http://localhost:3000/static/js/bundle.js:82996:12)
at m.info (http://localhost:3000/static/js/bundle.js:82805:26)
at Navbar (http://localhost:3000/static/js/bundle.js:1048:11)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

---

## 2.15. http://localhost:3000/privacy-policy

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/privacy-policy** |

### Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.search** and passed to **xhr.send**.

### Request

```
GET /privacy-policy HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:24 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

### Dynamic analysis

Data is read from **location.search** and passed to **xhr.send**.

The following value was injected into the source:

```
?vfc5jyc63s=vfc5jyc63s%27%22`'"/vfc5jyc63s/><vfc5jyc63s/\>oxsnkiq348&
```

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get search (<anonymous>:1:323065)
at Array.<anonymous> (http://localhost:3000/static/js/bundle.js:83675:84)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.addBaseInfo (http://localhost:3000/static/js/bundle.js:83670:13)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.ensureItemHasSomethingToSay (http://localhost:3000/static/js/bundle.js:83652:111)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleItemWithError (http://localhost:3000/static/js/bundle.js:83649:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleDomException (http://localhost:3000/static/js/bundle.js:83629:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at o._applyTransforms (http://localhost:3000/static/js/bundle.js:83257:7)
at o.log (http://localhost:3000/static/js/bundle.js:83245:12)
at a._log (http://localhost:3000/static/js/bundle.js:83025:202)
at a.info (http://localhost:3000/static/js/bundle.js:82996:12)
at m.info (http://localhost:3000/static/js/bundle.js:82805:26)
at Navbar (http://localhost:3000/static/js/bundle.js:1048:11)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
```

```
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

---

## 2.16. http://localhost:3000/privacy-policy

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/privacy-policy** |

### Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.href** and passed to **xhr.send**.

### Request

```
GET /privacy-policy HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:24 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

### Dynamic analysis

Data is read from **location.href** and passed to **xhr.send**.

The following value was injected into the source:

```
http://localhost:3000/privacy-policy?nzolhffxk9=nzolhffxk9%27%22`'"/nzolhffxk9/><nzolhffxk9/\>xv829q7igz&#nzolhffxk9=nzolhffxk9%27%22`'"/nzol
```

The previous value reached the sink as:

{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href (<anonymous>:1:323401)
at Array.<anonymous> (http://localhost:3000/static/js/bundle.js:83675:50)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.addBaseInfo (http://localhost:3000/static/js/bundle.js:83670:13)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.ensureItemHasSomethingToSay (http://localhost:3000/static/js/bundle.js:83652:111)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleItemWithError (http://localhost:3000/static/js/bundle.js:83649:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at Array.handleDomException (http://localhost:3000/static/js/bundle.js:83629:9)
at s (http://localhost:3000/static/js/bundle.js:83255:44)
at o._applyTransforms (http://localhost:3000/static/js/bundle.js:83257:7)
at o.log (http://localhost:3000/static/js/bundle.js:83245:12)
at a._log (http://localhost:3000/static/js/bundle.js:83025:202)
at a.info (http://localhost:3000/static/js/bundle.js:82996:12)
at m.info (http://localhost:3000/static/js/bundle.js:82805:26)
at Navbar (http://localhost:3000/static/js/bundle.js:1048:11)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

---

## 2.17. http://localhost:3000/privacy-policy

### Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/privacy-policy** |

### Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **document.cookie** and passed to **xhr.send**.

Because the data originates from a cookie, the application's behavior is not trivial to exploit in an attack against another user. Typically, you will need to find a means of setting an arbitrary cookie value in the victim's browser in order to exploit the vulnerability. Applications often contain "cookie-forcing" conditions which make this possible, and such a condition in any related domain or subdomain can potentially be used for this purpose. Nonetheless, this limitation somewhat mitigates the impact of the vulnerability.

### Request

```
GET /privacy-policy HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:24 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

## Dynamic analysis

Data is read from **document.cookie** and passed to **xhr.send**.

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object.<computed>.get (<anonymous>:1:624755)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99247:73)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61337:23)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

This was triggered by a **message** event.

---

# 2.18. http://localhost:3000/privacy-policy

## Summary

| | |
|---|---|
| Severity: | **Low** |
| Confidence: | **Tentative** |
| Host: | **http://localhost:3000** |
| Path: | **/privacy-policy** |

## Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **document.cookie** and passed to **xhr.send**.

Because the data originates from a cookie, the application's behavior is not trivial to exploit in an attack against another user. Typically, you will need to find a means of setting an arbitrary cookie value in the victim's browser in order to exploit the vulnerability. Applications often contain "cookie-forcing" conditions which make this possible, and such a condition in any related domain or subdomain can potentially be used for this purpose. Nonetheless, this limitation somewhat mitigates the impact of the vulnerability.

## Request

```
GET /privacy-policy HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:24 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

## Dynamic analysis

Data is read from **document.cookie** and passed to **xhr.send**.

The previous value reached the sink as:

```
{"data":{"environment":"dev","level":"info","endpoint":"api.rollbar.com/api/1/item/","platform":"browser","framework":"browser-js","language"
```

The stack trace at the source was:

```
at Object.<computed>.get (<anonymous>:1:624755)
at Cookies.update (http://localhost:3000/static/js/bundle.js:99247:73)
at Cookies.getAll (http://localhost:3000/static/js/bundle.js:99287:12)
at http://localhost:3000/static/js/bundle.js:98064:98
at mountState (http://localhost:3000/static/js/bundle.js:58574:24)
at Object.useState (http://localhost:3000/static/js/bundle.js:59179:20)
at useState (http://localhost:3000/static/js/bundle.js:81089:25)
at useCookies (http://localhost:3000/static/js/bundle.js:98064:83)
at useIsUserLoggedIn (http://localhost:3000/static/js/bundle.js:6167:85)
at AuthProvider (http://localhost:3000/static/js/bundle.js:384:101)
at renderWithHooks (http://localhost:3000/static/js/bundle.js:57995:22)
at mountIndeterminateComponent (http://localhost:3000/static/js/bundle.js:61279:17)
at beginWork (http://localhost:3000/static/js/bundle.js:62575:20)
at beginWork$1 (http://localhost:3000/static/js/bundle.js:67534:18)
at performUnitOfWork (http://localhost:3000/static/js/bundle.js:66804:16)
at workLoopSync (http://localhost:3000/static/js/bundle.js:66727:9)
at renderRootSync (http://localhost:3000/static/js/bundle.js:66700:11)
at performConcurrentWorkOnRoot (http://localhost:3000/static/js/bundle.js:66095:78)
at workLoop (http://localhost:3000/static/js/bundle.js:85224:38)
at flushWork (http://localhost:3000/static/js/bundle.js:85202:18)
at MessagePort.performWorkUntilDeadline (http://localhost:3000/static/js/bundle.js:85439:25)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.SHOuv (<anonymous>:1:178262)
at Object.qyGCn (<anonymous>:1:504610)
at Object.qumcA (<anonymous>:1:523851)
at _0x464a84.<computed>._0x902400.<computed>.<computed>.<computed> (<anonymous>:1:524455)
at XMLHttpRequest.<anonymous> (http://localhost:3000/static/js/bundle.js:84354:133)
at XMLHttpRequest.send (http://localhost:3000/static/js/bundle.js:84354:133)
at t.exports (http://localhost:3000/static/js/bundle.js:83556:226)
at s._makeRequest (http://localhost:3000/static/js/bundle.js:83473:45)
at s._makeZoneRequest (http://localhost:3000/static/js/bundle.js:83466:32)
at s.post (http://localhost:3000/static/js/bundle.js:83451:12)
at http://localhost:3000/static/js/bundle.js:83283:21
```

This was triggered by a **message** event.

---

# 3. Cross-origin resource sharing

There are 8 instances of this issue:

- /
- /about-us
- /manifest.json
- /privacy-policy
- /robots.txt
- /static/js/bundle.js
- /static/media/AppleWatch.7f761abd0b3972200451.pdf
- /static/media/Fitbit.7bf4ebbd1d8b1f4a61d0.pdf

## Issue background

An HTML5 cross-origin resource sharing (CORS) policy controls whether and how content running on other domains can perform two-way interaction with the domain that publishes the policy. The policy is fine-grained and can apply access controls per-request based on the URL and other features of the request.

If another domain is allowed by the policy, then that domain can potentially attack users of the application. If a user is logged in to the application, and visits a domain allowed by the policy, then any malicious content running on that domain can potentially retrieve content from the application, and sometimes carry out actions within the security context of the logged in user.

Even if an allowed domain is not overtly malicious in itself, security vulnerabilities within that domain could potentially be leveraged by an attacker to exploit the trust relationship and attack the application that allows access. CORS policies on pages containing sensitive information should be reviewed to determine whether it is appropriate for the application to trust both the intentions and security posture of any domains granted access.

## Issue remediation

Any inappropriate domains should be removed from the CORS policy.

## References

- Web Security Academy: Cross-origin resource sharing (CORS)
- Exploiting CORS Misconfigurations

## Vulnerability classifications

- CWE-942: Overly Permissive Cross-domain Whitelist

---

## 3.1. http://localhost:3000/

### Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/** |

### Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

### Request

```
GET / HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: http://localhost:3000
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
```

```
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:35:21 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

---

## 3.2. http://localhost:3000/about-us

### Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/about-us** |

### Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

### Request

```
GET /about-us HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: http://localhost:3000
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:35:43 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

---

## 3.3. http://localhost:3000/manifest.json

### Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/manifest.json** |

### Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

## Request

```
GET /manifest.json HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
Origin: http://localhost:3000
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Mon, 01 Apr 2024 00:07:13 GMT
ETag: W/"126-18e96fb46d1"
Content-Type: application/json; charset=UTF-8
Content-Length: 294
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:35:08 GMT
Connection: close

{
"short_name": "BEAPEngine",
"name": "BEAPEngine",
"icons": [
{
"src": "beap_lab_hex_small.png",
"type": "image/png",
"sizes": "512x512 192x192"
}
],
"start_url":
...[SNIP]...
```

---

# 3.4. http://localhost:3000/privacy-policy

## Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/privacy-policy** |

## Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

## Request

```
GET /privacy-policy HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

```
Content-Length: 0
Origin: http://localhost:3000
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:35:18 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

---

# 3.5. http://localhost:3000/robots.txt

## Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/robots.txt** |

## Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

## Request

```
GET /robots.txt HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: http://localhost:3000
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Fri, 29 Mar 2024 20:41:58 GMT
ETag: W/"43-18e8bf2a428"
Content-Type: text/plain; charset=UTF-8
Content-Length: 67
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:34:49 GMT
Connection: close

# https://www.robotstxt.org/robotstxt.html
User-agent: *
Disallow:
```

---

# 3.6. http://localhost:3000/static/js/bundle.js

## Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/static/js/bundle.js** |

## Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

## Request

```
GET /static/js/bundle.js HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
Origin: http://localhost:3000
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: application/javascript; charset=utf-8
Accept-Ranges: bytes
ETag: W/"439b8c-1eh3Waf3Rr2nQhZqgwvsyoxEGzE"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:35:44 GMT
Connection: close
Content-Length: 4430732

/******/ (() => { // webpackBootstrap
/******/ 	var __webpack_modules__ = ({

/***/ "./src/App.tsx":
/*!*********************!*\
!*** ./src/App.tsx ***!
\*********************/
/***/ ((module, __w
...[SNIP]...
```

---

# 3.7. http://localhost:3000/static/media/AppleWatch.7f761abd0b3972200451.pdf

## Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/static/media/AppleWatch.7f761abd0b3972200451.pdf** |

## Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

## Request

```
GET /static/media/AppleWatch.7f761abd0b3972200451.pdf HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

```
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
Origin: http://localhost:3000
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: application/pdf
Accept-Ranges: bytes
Content-Length: 798604
ETag: W/"c2f8c-A7NCPrGH4UpL7mNpneDWTnG6EYY"
Date: Thu, 04 Apr 2024 01:35:32 GMT
Connection: close

%PDF-1.3
%.....
4 0 obj
<< /Length 5 0 R /Filter /FlateDecode >>
stream
x..V.n.1...+*@H7!.....'.Z.@8.QP@.....&!4..].?..^..'...$%.A.6.....erqJ....^\JZ_...  h.i. 3:.%.rL|j...'N.`p..;.4.
...[SNIP]...
```

---

# 3.8. http://localhost:3000/static/media/Fitbit.7bf4ebbd1d8b1f4a61d0.pdf

## Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/static/media/Fitbit.7bf4ebbd1d8b1f4a61d0.pdf** |

## Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

## Request

```
GET /static/media/Fitbit.7bf4ebbd1d8b1f4a61d0.pdf HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
Origin: http://localhost:3000
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: application/pdf
Accept-Ranges: bytes
Content-Length: 794418
ETag: W/"c1f32-5dkX4JA3U689Sr9yAsqxJL7lEU8"
Date: Thu, 04 Apr 2024 01:35:32 GMT
Connection: close

%PDF-1.3
%.....
4 0 obj
<< /Length 5 0 R /Filter /FlateDecode >>
stream
x..WK..5...WT2a.....
```

p..H#q`9..F.....\v.L.cw.j..]...>..'zO...M..8...a.>.....7....d.....@.!.g.~...d.....!e.
**...[SNIP]...**

# 4. Cross-origin resource sharing: arbitrary origin trusted

There are 8 instances of this issue:

- /
- /about-us
- /manifest.json
- /privacy-policy
- /robots.txt
- /static/js/bundle.js
- /static/media/AppleWatch.7f761abd0b3972200451.pdf
- /static/media/Fitbit.7bf4ebbd1d8b1f4a61d0.pdf

## Issue background

An HTML5 cross-origin resource sharing (CORS) policy controls whether and how content running on other domains can perform two-way interaction with the domain that publishes the policy. The policy is fine-grained and can apply access controls per-request based on the URL and other features of the request.

Trusting arbitrary origins effectively disables the same-origin policy, allowing two-way interaction by third-party web sites. Unless the response consists only of unprotected public content, this policy is likely to present a security risk.

If the site specifies the header Access-Control-Allow-Credentials: true, third-party sites may be able to carry out privileged actions and retrieve sensitive information. Even if it does not, attackers may be able to bypass any IP-based access controls by proxying through users' browsers.

## Issue remediation

Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.

## References

- Web Security Academy: Cross-origin resource sharing (CORS)
- Exploiting CORS Misconfigurations

## Vulnerability classifications

- CWE-942: Overly Permissive Cross-domain Whitelist

---

## 4.1. http://localhost:3000/

### Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/** |

### Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **http://eywbhlsrvqmx.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

### Request

```
GET / HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: http://eywbhlsrvqmx.com
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:35:22 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

---

## 4.2. http://localhost:3000/about-us

### Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/about-us** |

### Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **http://ghveogouuifw.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

### Request

```
GET /about-us HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: http://ghveogouuifw.com
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:35:49 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

---

## 4.3. http://localhost:3000/manifest.json

### Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |

| | |
|---|---|
| Host: | **http://localhost:3000** |
| Path: | **/manifest.json** |

## Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **http://knijhmfvarme.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

## Request

```
GET /manifest.json HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
Origin: http://knijhmfvarme.com
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Mon, 01 Apr 2024 00:07:13 GMT
ETag: W/"126-18e96fb46d1"
Content-Type: application/json; charset=UTF-8
Content-Length: 294
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:35:14 GMT
Connection: close

{
"short_name": "BEAPEngine",
"name": "BEAPEngine",
"icons": [
{
"src": "beap_lab_hex_small.png",
"type": "image/png",
"sizes": "512x512 192x192"
}
],
"start_url":
...[SNIP]...
```

---

# 4.4. http://localhost:3000/privacy-policy

## Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/privacy-policy** |

## Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **http://wqfazezubexe.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

## Request

```
GET /privacy-policy HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
Origin: http://wqfazezubexe.com
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:35:19 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

---

# 4.5. http://localhost:3000/robots.txt

## Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/robots.txt** |

## Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **http://dgtjatlufhyd.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

## Request

```
GET /robots.txt HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: http://dgtjatlufhyd.com
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Fri, 29 Mar 2024 20:41:58 GMT
ETag: W/"43-18e8bf2a428"
Content-Type: text/plain; charset=UTF-8
Content-Length: 67
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:34:49 GMT
Connection: close

# https://www.robotstxt.org/robotstxt.html
```

```
User-agent: *
Disallow:
```

## 4.6. http://localhost:3000/static/js/bundle.js

### Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/static/js/bundle.js** |

### Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **http://ksxmjfnsswcc.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

### Request

```
GET /static/js/bundle.js HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
Origin: http://ksxmjfnsswcc.com
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: application/javascript; charset=utf-8
Accept-Ranges: bytes
ETag: W/"439b8c-1eh3Waf3Rr2nQhZqgwvsyoxEGzE"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:35:46 GMT
Connection: close
Content-Length: 4430732

/******/ (() => { // webpackBootstrap
/******/ 	var __webpack_modules__ = ({

/***/ "./src/App.tsx":
/*!*********************!*\
!*** ./src/App.tsx ***!
\*********************/
/***/ ((module, __w
...[SNIP]...
```

## 4.7. http://localhost:3000/static/media/AppleWatch.7f761abd0b3972200451.pdf

### Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/static/media/AppleWatch.7f761abd0b3972200451.pdf** |

### Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **http://weqmekycyzqo.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

## Request

```
GET /static/media/AppleWatch.7f761abd0b3972200451.pdf HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
Origin: http://weqmekycyzqo.com
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: application/pdf
Accept-Ranges: bytes
Content-Length: 798604
ETag: W/"c2f8c-A7NCPrGH4UpL7mNpneDWTnG6EYY"
Date: Thu, 04 Apr 2024 01:35:32 GMT
Connection: close

%PDF-1.3
%.....
4 0 obj
<< /Length 5 0 R /Filter /FlateDecode >>
stream
x..V.n.1...+*@H7!.....'.Z.@8.QP@.....&!4..].?..^..'...$%.A.6.....erqJ....^\JZ_...  h.i. 3:.%.rL|j...'N.`p..;.4.
...[SNIP]...
```

---

# 4.8. http://localhost:3000/static/media/Fitbit.7bf4ebbd1d8b1f4a61d0.pdf

## Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/static/media/Fitbit.7bf4ebbd1d8b1f4a61d0.pdf** |

## Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **http://fjgbapefzcmt.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

## Request

```
GET /static/media/Fitbit.7bf4ebbd1d8b1f4a61d0.pdf HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
Origin: http://fjgbapefzcmt.com
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: application/pdf
Accept-Ranges: bytes
Content-Length: 794418
ETag: W/"c1f32-5dkX4JA3U689Sr9yAsqxJL7lEU8"
Date: Thu, 04 Apr 2024 01:35:32 GMT
Connection: close

%PDF-1.3
%.....
4 0 obj
<< /Length 5 0 R /Filter /FlateDecode >>
stream
x..WK..5...WT2a.....
p..H#q`9..F.....\v.L.cw.j..]...>...'zO...M..8...a.>.....7....d.....@.!.g.~...d.....!e.
...[SNIP]...
```

# 5. Frameable response (potential Clickjacking)

There are 2 instances of this issue:

- /about-us
- /privacy-policy

## Issue description

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

## Issue remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

## References

- Web Security Academy: Clickjacking
- X-Frame-Options

## Vulnerability classifications

- CWE-693: Protection Mechanism Failure
- CWE-1021: Improper Restriction of Rendered UI Layers or Frames
- CAPEC-103: Clickjacking

---

## 5.1. http://localhost:3000/about-us

### Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Firm** |
| Host: | **http://localhost:3000** |
| Path: | **/about-us** |

### Request

```
GET /about-us HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
```

```
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:28 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

## 5.2. http://localhost:3000/privacy-policy

### Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Firm** |
| Host: | **http://localhost:3000** |
| Path: | **/privacy-policy** |

### Request

```
GET /privacy-policy HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:24 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
```

# 6. Private IP addresses disclosed

There are 2 instances of this issue:

- /about-us
- /privacy-policy

### Issue background

RFC 1918 specifies ranges of IP addresses that are reserved for use in private networks and cannot be routed on the public Internet. Although various methods exist by which an attacker can determine the public IP addresses in use by an organization, the private addresses used internally cannot usually be determined in the same ways.

Discovering the private addresses used within an organization can help an attacker in carrying out network-layer attacks aiming to penetrate the organization's internal infrastructure.

## Issue remediation

There is not usually any good reason to disclose the internal IP addresses used within an organization's infrastructure. If these are being returned in service banners or debug messages, then the relevant services should be configured to mask the private addresses. If they are being used to track back-end servers for load balancing purposes, then the addresses should be rewritten with innocuous identifiers from which an attacker cannot infer any useful information about the infrastructure.

## References

- Web Security Academy: Information disclosure

## Vulnerability classifications

- CWE-200: Information Exposure
- CAPEC-37: Retrieve Embedded Sensitive Data

---

# 6.1. http://localhost:3000/about-us

## Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/about-us** |

## Issue detail

The following RFC 1918 IP addresses were disclosed in the response:

- 10.0.0.248
- 172.18.0.1

## Request

```
GET /about-us HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:28 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
5234XlJqIg','__es'+'Module','_allowedToConnectOnSend','ws://','send','error','_connectAttemptCount','91jexGAm','_ws','env','stringify',
[\"localhost\",\"127.0.0.1\",\"example.cypress.io\",\"GlennOS\",\"10.0.0.248\",\"172.18.0.1\"],'location','1.0.0','Unknown\\x20error','onerror','4777448DoNeqc','127.0.0.1','node','getOwnProperty
Names','then','data','gateway.docker.internal','\\x20browser','_WebSocketClass','failed\\x20to\\x2
...[SNIP]...
```

---

# 6.2. http://localhost:3000/privacy-policy

### Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/privacy-policy** |

### Issue detail

The following RFC 1918 IP addresses were disclosed in the response:

- 10.0.0.248
- 172.18.0.1

### Request

```
GET /privacy-policy HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://localhost:3000/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
ETag: W/"36b9-MJaGmruv93asyHCM4bLub6uFyDk"
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:33:24 GMT
Connection: close
Content-Length: 14009

<!DOCTYPE html>
<html lang="en">
<head><script>try{(0,eval)("globalThis._triedToInstallGlobalErrorHandler") || (0,eval)("/* https://github.com/wallabyjs/console-ninja#how-does-it-work */'use strict'
...[SNIP]...
5234XlJqlg','__es'+'Module','_allowedToConnectOnSend','ws://','send','error','_connectAttemptCount','91jexGAm','_ws','env','stringify',
[\"localhost\",\"127.0.0.1\",\"example.cypress.io\",\"GlennOS\",\"10.0.0.248\",\"172.18.0.1\"],'location','1.0.0','Unknown\\x20error','onerror','4777448DoNeqc','127.0.0.1','node','getOwnPropertyNames','then','data','gateway.docker.internal','\\x20browser','_WebSocketClass','failed\\x20to\\x2
...[SNIP]...
```

## 7. Robots.txt file

### Summary

| | |
|---|---|
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **http://localhost:3000** |
| Path: | **/robots.txt** |

### Issue detail

The web server contains a robots.txt file.

### Issue background

The file robots.txt is used to give instructions to web robots, such as search engine crawlers, about locations within the web site that robots are allowed, or not allowed, to crawl and index.

The presence of the robots.txt does not in itself present any kind of security vulnerability. However, it is often used to identify restricted or private areas of a site's contents. The information in the file may therefore help an attacker to map out the site's contents, especially if some of the locations identified are not linked from elsewhere in the site. If the application relies on robots.txt to protect access to these areas, and does not enforce proper access control over them, then this presents a serious vulnerability.

### Issue remediation

The robots.txt file is not itself a security threat, and its correct use can represent good practice for non-security reasons. You should not assume that all web robots will honor the file's instructions. Rather, assume that attackers will pay close attention to any locations identified in the file. Do not rely on robots.txt to provide any kind of protection over unauthorized access.

## Vulnerability classifications

- CWE-200: Information Exposure

## Request

```
GET /robots.txt HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

## Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Fri, 29 Mar 2024 20:41:58 GMT
ETag: W/"43-18e8bf2a428"
Content-Type: text/plain; charset=UTF-8
Content-Length: 67
Vary: Accept-Encoding
Date: Thu, 04 Apr 2024 01:34:48 GMT
Connection: close

# https://www.robotstxt.org/robotstxt.html
User-agent: *
Disallow:
```

---

Report generated by Burp Suite web vulnerability scanner v2024.2.1.3, at Wed Apr 03 19:58:36 CST 2024.