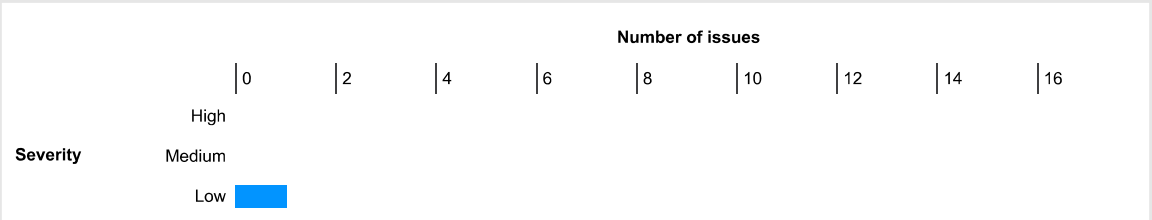
Burp Scanner Report

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	1	0	0	1
	Information	10	8	0	18
	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. Strict transport security not enforced

2. Frameable response (potential Clickjacking)

3. DOM data manipulation (DOM-based)

3.1. https://okx2222.com/
3.2. https://okx2222.com/
3.3. https://okx2222.com/
3.4. https://okx2222.com/
3.5. https://okx2222.com/
3.6. https://okx2222.com/
3.7. https://okx2222.com/

4. Cacheable HTTPS response

4.1. https://okx2222.com/
4.2. https://okx2222.com/api/chain/getOpenCurrencyList
4.3. https://okx2222.com/api/common/getAppConfigAndCompanyConfig
4.4. https://okx2222.com/api/common/getCustomerServiceConfig
4.5. https://okx2222.com/api/common/getExplainList
4.6. https://okx2222.com/api/common/getProductList
4.7. https://okx2222.com/api/common/getSlide
4.8. https://okx2222.com/api/common/pageNotice
4.9. https://okx2222.com/static/js/pages-home-index.d13e0d47.js

5. TLS certificate

1. Strict transport security not enforced

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://okx2222.com**

Path: **/**

Issue detail

This issue was found in multiple locations under the reported path.

Issue background

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability classifications

- CWE-523: Unprotected Transport of Credentials
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

Request

```
GET / HTTP/1.1
Host: okx2222.com
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/123.0.6312.122 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/2 200 OK
Date: Wed, 01 May 2024 04:29:24 GMT
Content-Type: text/html
Last-Modified: Fri, 26 Apr 2024 12:27:45 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=nuW71HmiieFuShjGTNBnBni%2BpzM9lOVfTeENNzgEvp4MgCcMVWSHUWzYCYOXo%2BcmIrBFEt4Rt8mjIloBRCl4PXl52SPfXfmP6Xf0SyaG15FzL9AZp1Izglgko%2FM4YA%3D
%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd07c378b39c45-SIN
Alt-Svc: h3=":443"; ma=86400

<!DOCTYPE html><html lang=zh-CN><head><meta charset=utf-8><meta http-equiv=X-UA-Compatible content="IE=edge"><link rel="shortcut icon" type=image/x-icon
href=/static/icon.png?11><meta name=viewport co
...[SNIP]...
```

---

2. Frameable response (potential Clickjacking)

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://okx2222.com**
Path:	**/**

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

Request

```
GET / HTTP/1.1
Host: okx2222.com
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/123.0.6312.122 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/2 200 OK
Date: Wed, 01 May 2024 04:29:24 GMT
Content-Type: text/html
Last-Modified: Fri, 26 Apr 2024 12:27:45 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=nuW71HmiieFuShjGTNBnBni%2BpzM9lOVfTeENNzgEvp4MgCcMVWSHUWzYCYOXo%2BcmlrBFEt4Rt8mjIIoBRCl4PXI52SPfXfmP6Xf0SyaG15FzL9AZp1Izglgko%2FM4YA%3D
%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd07c378b39c45-SIN
Alt-Svc: h3=":443"; ma=86400

<!DOCTYPE html><html lang=zh-CN><head><meta charset=utf-8><meta http-equiv=X-UA-Compatible content="IE=edge"><link rel="shortcut icon" type=image/x-icon
href=/static/icon.png?11><meta name=viewport co
...[SNIP]...
```

---

3. DOM data manipulation (DOM-based)

There are 7 instances of this issue:

- /
- /
- /
- /
- /
- /
- /

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 data manipulation arises when a script writes controllable data to a field within the DOM that is used within the visible UI or client-side application logic. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the appearance or behavior of the client-side UI. An attacker may be able to leverage this to perform virtual defacement of the application, or possibly to induce the user to perform unintended actions.

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 DOM data manipulation vulnerabilities is not to dynamically write to DOM data fields any 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 being stored. In general, this is best achieved by using a whitelist of permitted values.

References

- Web Security Academy: DOM data manipulation

Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

3.1. https://okx2222.com/

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://okx2222.com**
Path:	**/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.href** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: okx2222.com
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/123.0.6312.122 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/2 200 OK
Date: Wed, 01 May 2024 04:29:24 GMT
Content-Type: text/html
Last-Modified: Fri, 26 Apr 2024 12:27:45 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=nuW71HmiieFuShjGTNBnBni%2BpzM9lOVfTeENNzgEvp4MgCcMVWSHUWzYCYOXo%2BcmIrBFEt4Rt8mjIloBRCl4PXI52SPfXfmP6Xf0SyaG15FzL9AZp1Izglgko%2FM4YA%3D
%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd07c378b39c45-SIN
Alt-Svc: h3=":443"; ma=86400

<!DOCTYPE html><html lang=zh-CN><head><meta charset=utf-8><meta http-equiv=X-UA-Compatible content="IE=edge"><link rel="shortcut icon" type=image/x-icon
href=/static/icon.png?11><meta name=viewport co
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **history.replaceState.**

The following value was injected into the source:

```
https://okx2222.com/?w8fuhri0nu=w8fuhri0nu%27%22`'"/w8fuhri0nu/><w8fuhri0nu/\>l8bekmj3ho&#w8fuhri0nu=w8fuhri0nu%27%22`'"/w8fuhri0nu/><w8fuhri0nu/\>l8b
```

The previous value reached the sink as:

```
https://okx2222.com/?oniis3f291=oniis3f291%27%22`'"/oniis3f291/><oniis3f291/\>hd4a8ne2p4&#/w8fuhri0nu=w8fuhri0nu'"`'"/w8fuhri0nu/><w8fuhri0nu/\>l8bekm
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href (<anonymous>:1:323401)
at ne (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149773)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149692)
at new e (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:148039)
at new se (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151248)
at Object.install (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:163805)
at Sr.t.use (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36359)
at i.value (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:106442)
at new i (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:105955)
at Object.<anonymous> (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:106609)
at 2ef3 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:106617)
at n (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16188)
at Module.fae3 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:499371)
at n (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16188)
at 0001 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16992)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:17006
at 0001 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:15990)
at 1c31 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16023)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73098)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at t (https://okx2222.com/static/js/index.247330ad.js:1:431)
at https://okx2222.com/static/js/index.247330ad.js:1:8503
at https://okx2222.com/static/js/index.247330ad.js:1:8508
```

The stack trace at the sink was:

```
at Object.AdTdD (<anonymous>:1:618162)
at History.replaceState (<anonymous>:1:618402)
at Pt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142003)
at Mt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142146)
at oe (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:150006)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149723)
at new e (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:148039)
at new se (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151248)
at Object.install (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:163805)
at Sr.t.use (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36359)
at i.value (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:106442)
at new i (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:105955)
at Object.<anonymous> (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:106609)
at 2ef3 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:106617)
at n (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16188)
at Module.fae3 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:499371)
at n (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16188)
at 0001 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16992)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:17006
at 0001 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:15990)
at 1c31 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16023)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73098)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at t (https://okx2222.com/static/js/index.247330ad.js:1:431)
at https://okx2222.com/static/js/index.247330ad.js:1:8503
at https://okx2222.com/static/js/index.247330ad.js:1:8508
```

3.2. https://okx2222.com/

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://okx2222.com**
Path:	**/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.href** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: okx2222.com
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/123.0.6312.122 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/2 200 OK
Date: Wed, 01 May 2024 04:29:24 GMT
Content-Type: text/html
Last-Modified: Fri, 26 Apr 2024 12:27:45 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=nuW71HmiieFuShjGTNBnBni%2BpzM9lOVfTeENNzgEvp4MgCcMVWSHUWzYCYOXo%2BcmIrBFEt4Rt8mjIIoBRCl4PXI52SPfXfmP6Xf0SyaG15FzL9AZp1IzgIgko%2FM4YA%3D
%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd07c378b39c45-SIN
Alt-Svc: h3=":443"; ma=86400

<!DOCTYPE html><html lang=zh-CN><head><meta charset=utf-8><meta http-equiv=X-UA-Compatible content="IE=edge"><link rel="shortcut icon" type=image/x-icon
href=/static/icon.png?11><meta name=viewport co
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **history.replaceState.**

The following value was injected into the source:

```
https://okx2222.com/?oniis3f291=oniis3f291%27%22`'"/oniis3f291/><oniis3f291/\>hd4a8ne2p4&#oniis3f291=oniis3f291%27%22`'"/oniis3f291/><oniis3f291/\>hd4
```

The previous value reached the sink as:

```
https://okx2222.com/?oniis3f291=oniis3f291%27%22`'"/oniis3f291/><oniis3f291/\>hd4a8ne2p4&#/w8fuhri0nu=w8fuhri0nu'"`'"/w8fuhri0nu/><w8fuhri0nu/\>l8bekm
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href (<anonymous>:1:323401)
at re (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149872)
at oe (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:150009)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149723)
at new e (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:148039)
at new se (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151248)
at Object.install (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:163805)
at Sr.t.use (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36359)
at i.value (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:106442)
at new i (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:105955)
at Object.<anonymous> (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:106609)
at 2ef3 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:106617)
at n (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16188)
at Module.fae3 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:499371)
at n (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16188)
at 0001 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16992)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:17006
at 0001 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:15990)
at 1c31 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16023)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73098)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at t (https://okx2222.com/static/js/index.247330ad.js:1:431)
at https://okx2222.com/static/js/index.247330ad.js:1:8503
at https://okx2222.com/static/js/index.247330ad.js:1:8508
```

The stack trace at the sink was:

```
at Object.AdTdD (<anonymous>:1:618162)
at History.replaceState (<anonymous>:1:618402)
at Pt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142003)
at Mt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142146)
at oe (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:150006)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149723)
at new e (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:148039)
at new se (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151248)
at Object.install (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:163805)
at Sr.t.use (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36359)
at i.value (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:106442)
at new i (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:105955)
at Object.<anonymous> (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:106609)
at 2ef3 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:106617)
at n (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16188)
at Module.fae3 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:499371)
at n (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16188)
at 0001 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16992)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:17006
at 0001 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:15990)
at 1c31 (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:1:16023)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73098)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at t (https://okx2222.com/static/js/index.247330ad.js:1:431)
at https://okx2222.com/static/js/index.247330ad.js:1:8503
at https://okx2222.com/static/js/index.247330ad.js:1:8508
```

3.3. https://okx2222.com/

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://okx2222.com**
Path:	**/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.href** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: okx2222.com
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/123.0.6312.122 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/2 200 OK
Date: Wed, 01 May 2024 04:29:24 GMT
```

```
Content-Type: text/html
Last-Modified: Fri, 26 Apr 2024 12:27:45 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=nuW71HmiieFuShjGTNBnBni%2BpzM9IOVfTeENNzgEvp4MgCcMVWSHUWzYCYOXo%2BcmlrBFEt4Rt8mjIloBRCI4PXI52SPfXfmP6Xf0SyaG15FzL9AZp1IzgIgko%2FM4YA%3D
%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd07c378b39c45-SIN
Alt-Svc: h3=":443"; ma=86400

<!DOCTYPE html><html lang=zh-CN><head><meta charset=utf-8><meta http-equiv=X-UA-Compatible content="IE=edge"><link rel="shortcut icon" type=image/x-icon
href=/static/icon.png?11><meta name=viewport co
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **history.replaceState.**

The following value was injected into the source:

```
https://okx2222.com/?nu2fvtcmbi=nu2fvtcmbi%27%22`'"/nu2fvtcmbi/><nu2fvtcmbi/\>kv484ia6ja&#nu2fvtcmbi=nu2fvtcmbi%27%22`'"/nu2fvtcmbi/><nu2fvtcmbi/\>kv4
```

The previous value reached the sink as:

```
/?nu2fvtcmbi=nu2fvtcmbi%27%22`'"/nu2fvtcmbi/><nu2fvtcmbi/\>kv484ia6ja&#nu2fvtcmbi=nu2fvtcmbi%27%22`'"/nu2fvtcmbi/><nu2fvtcmbi/\>kv484ia6ja&
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href (<anonymous>:1:323401)
at vt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:140385)
at e.setupListeners (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:148239)
at i (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151931)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:144895
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145933
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142206)
at It (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142252)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145871
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142206)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142234
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145738
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142770
at h (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145528)
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142215)
at It (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142252)
at Ht.confirmTransition (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145762)
at Ht.transitionTo (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:144843)
at se.init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151951)
at xr.beforeCreate (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:132046)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:11940)
at Dn (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:29997)
at t._init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:35336)
at new xr (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36144)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73458)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at t (https://okx2222.com/static/js/index.247330ad.js:1:431)
```

The stack trace at the sink was:

```
at Object.AdTdD (<anonymous>:1:618162)
at History.replaceState (<anonymous>:1:618402)
at vt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:140288)
at e.setupListeners (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:148239)
at i (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151931)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:144895
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145933
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142206)
at It (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142252)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145871
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142206)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142234
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145738
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142770
at h (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145528)
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142215)
at It (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142252)
at Ht.confirmTransition (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145762)
at Ht.transitionTo (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:144843)
at se.init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151951)
at xr.beforeCreate (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:132046)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:11940)
at Dn (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:29997)
at t._init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:35336)
at new xr (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36144)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73458)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at t (https://okx2222.com/static/js/index.247330ad.js:1:431)
```

3.4. https://okx2222.com/

Summary

Severity: **Information**

Confidence: **Firm**

Host: **https://okx2222.com**

Path: **/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.href** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: okx2222.com
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/123.0.6312.122 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/2 200 OK
Date: Wed, 01 May 2024 04:29:24 GMT
Content-Type: text/html
Last-Modified: Fri, 26 Apr 2024 12:27:45 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=nuW71HmiieFuShjGTNBnBni%2BpzM9lOVfTeENNzgEvp4MgCcMVWSHUWzYCYOXo%2BcmlrBFEt4Rt8mjIloBRCl4PXI52SPfXfmP6Xf0SyaG15FzL9AZp1IzgIgko%2FM4YA%3D
%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd07c378b39c45-SIN
Alt-Svc: h3=":443"; ma=86400

<!DOCTYPE html><html lang=zh-CN><head><meta charset=utf-8><meta http-equiv=X-UA-Compatible content="IE=edge"><link rel="shortcut icon" type=image/x-icon
href=/static/icon.png?11><meta name=viewport co
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **history.replaceState.**

The following value was injected into the source:

```
https://okx2222.com/?elb5f3kk1o=elb5f3kk1o%27%22`'"/elb5f3kk1o/><elb5f3kk1o/\>bdwkh2ujmk&#elb5f3kk1o=elb5f3kk1o%27%22`'"/elb5f3kk1o/><elb5f3kk1o/\>bdw
```

The previous value reached the sink as:

```
https://okx2222.com/?dmev7dxstn=dmev7dxstn%27%22`'"/dmev7dxstn/><dmev7dxstn/\>vwk7jai3li&#/elb5f3kk1o=elb5f3kk1o'"`'"/elb5f3kk1o/><elb5f3kk1o/\>bdwkh2
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href (<anonymous>:1:323401)
at ne (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149773)
at e.getCurrentLocation (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149532)
at se.init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151966)
at xr.beforeCreate (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:132046)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:11940)
at Dn (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:29997)
at t._init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:35336)
at new xr (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36144)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73458)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at t (https://okx2222.com/static/js/index.247330ad.js:1:431)
at https://okx2222.com/static/js/index.247330ad.js:1:8503
at https://okx2222.com/static/js/index.247330ad.js:1:8508
```

The stack trace at the sink was:

```
at Object.AdTdD (<anonymous>:1:618162)
at History.replaceState (<anonymous>:1:618402)
at Pt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142003)
at Mt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142146)
at oe (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:150006)
at e.ensureURL (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149443)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:144902
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145933
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142206)
at It (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142252)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145871
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142206)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142234
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145738
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142770
at h (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145528)
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142215)
at It (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142252)
```

```
at Ht.confirmTransition (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145762)
at Ht.transitionTo (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:144843)
at se.init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151951)
at xr.beforeCreate (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:132046)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:11940)
at Dn (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:29997)
at t._init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:35336)
at new xr (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36144)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73458)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
```

3.5. https://okx2222.com/

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://okx2222.com**
Path:	**/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.href** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: okx2222.com
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/123.0.6312.122 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/2 200 OK
Date: Wed, 01 May 2024 04:29:24 GMT
Content-Type: text/html
Last-Modified: Fri, 26 Apr 2024 12:27:45 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=nuW71HmiieFuShjGTNBnBni%2BpzM9lOVfTeENNzgEvp4MgCcMVWSHUWzYCYOXo%2BcmlrBFEt4Rt8mjIloBRCl4PXl52SPfXfmP6Xf0SyaG15FzL9AZp1IzgIgko%2FM4YA%3D
%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd07c378b39c45-SIN
Alt-Svc: h3=":443"; ma=86400

<!DOCTYPE html><html lang=zh-CN><head><meta charset=utf-8><meta http-equiv=X-UA-Compatible content="IE=edge"><link rel="shortcut icon" type=image/x-icon
href=/static/icon.png?11><meta name=viewport co
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **history.replaceState.**

The following value was injected into the source:

```
https://okx2222.com/?dmev7dxstn=dmev7dxstn%27%22`'"/dmev7dxstn/><dmev7dxstn/\>vwk7jai3li&#dmev7dxstn=dmev7dxstn%27%22`'"/dmev7dxstn/><dmev7dxstn/\>vwk
```

The previous value reached the sink as:

```
https://okx2222.com/?dmev7dxstn=dmev7dxstn%27%22`'"/dmev7dxstn/><dmev7dxstn/\>vwk7jai3li&#/elb5f3kk1o=elb5f3kk1o'"`'"/elb5f3kk1o/><elb5f3kk1o/\>bdwkh2
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href (<anonymous>:1:323401)
at re (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149872)
at oe (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:150009)
at e.ensureURL (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149443)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:144902
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145933
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142206)
at It (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142252)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145871
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142206)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142234
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145738
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142770
at h (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145528)
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142215)
at It (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142252)
```

```
at Ht.confirmTransition (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145762)
at Ht.transitionTo (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:144843)
at se.init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151951)
at xr.beforeCreate (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:132046)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:11940)
at Dn (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:29997)
at t._init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:35336)
at new xr (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36144)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73458)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at t (https://okx2222.com/static/js/index.247330ad.js:1:431)
```

The stack trace at the sink was:

```
at Object.AdTdD (<anonymous>:1:618162)
at History.replaceState (<anonymous>:1:618402)
at Pt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142003)
at Mt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142146)
at oe (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:150006)
at e.ensureURL (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149443)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:144902
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145933
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142206)
at It (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142252)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145871
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142206)
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142234
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145738
at https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142770
at h (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145528)
at r (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142215)
at It (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142252)
at Ht.confirmTransition (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:145762)
at Ht.transitionTo (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:144843)
at se.init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151951)
at xr.beforeCreate (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:132046)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:11940)
at Dn (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:29997)
at t._init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:35336)
at new xr (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36144)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73458)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
```

3.6. https://okx2222.com/

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://okx2222.com**
Path:	**/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.href** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: okx2222.com
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/123.0.6312.122 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/2 200 OK
Date: Wed, 01 May 2024 04:29:24 GMT
Content-Type: text/html
Last-Modified: Fri, 26 Apr 2024 12:27:45 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=nuW71HmiieFuShjGTNBnBni%2BpzM9lOVfTeENNzgEvp4MgCcMVWSHUWzYCYOXo%2BcmlrBFEt4Rt8mjIIoBRCl4PXI52SPfXfmP6Xf0SyaG15FzL9AZp1Izglgko%2FM4YA%3D
%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd07c378b39c45-SIN
Alt-Svc: h3=":443"; ma=86400

<!DOCTYPE html><html lang=zh-CN><head><meta charset=utf-8><meta http-equiv=X-UA-Compatible content="IE=edge"><link rel="shortcut icon" type=image/x-icon
href=/static/icon.png?11><meta name=viewport co
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **history.replaceState.**

The following value was injected into the source:

```
https://okx2222.com/?fw17e44419=fw17e44419%27%22`'"/fw17e44419/><fw17e44419/\>ej3wvnyaup&#fw17e44419=fw17e44419%27%22`'"/fw17e44419/><fw17e44419/\>ej3
```

The previous value reached the sink as:

```
https://okx2222.com/?p4iyoobk0n=p4iyoobk0n%27%22`'"/p4iyoobk0n/><p4iyoobk0n/\>rdoydb0g4e&#/fw17e44419=fw17e44419'"`'"/fw17e44419/><fw17e44419/\>ej3wvn
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href (<anonymous>:1:323401)
at ne (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149773)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149692)
at new e (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:148039)
at new se (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151248)
at i (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:185697)
at k (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:185770)
at l (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:90562)
at xr.beforeCreate (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:160806)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:11940)
at Dn (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:29997)
at t._init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:35336)
at new xr (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36144)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73458)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at t (https://okx2222.com/static/js/index.247330ad.js:1:431)
at https://okx2222.com/static/js/index.247330ad.js:1:8503
at https://okx2222.com/static/js/index.247330ad.js:1:8508
```

The stack trace at the sink was:

```
at Object.AdTdD (<anonymous>:1:618162)
at History.replaceState (<anonymous>:1:618402)
at Pt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142003)
at Mt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142146)
at oe (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:150006)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149723)
at new e (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:148039)
at new se (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151248)
at i (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:185697)
at k (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:185770)
at l (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:90562)
at xr.beforeCreate (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:160806)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:11940)
at Dn (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:29997)
at t._init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:35336)
at new xr (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36144)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73458)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at t (https://okx2222.com/static/js/index.247330ad.js:1:431)
at https://okx2222.com/static/js/index.247330ad.js:1:8503
at https://okx2222.com/static/js/index.247330ad.js:1:8508
```

3.7. https://okx2222.com/

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://okx2222.com**
Path:	**/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.href** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: okx2222.com
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/123.0.6312.122 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/2 200 OK
Date: Wed, 01 May 2024 04:29:24 GMT
Content-Type: text/html
Last-Modified: Fri, 26 Apr 2024 12:27:45 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=nuW71HmiieFuShjGTNBnBni%2BpzM9lOVfTeENNzgEvp4MgCcMVWSHUWzYCYOXo%2BcmIrBFEt4Rt8mjIIoBRCI4PXI52SPfXfmP6Xf0SyaG15FzL9AZp1IzgIgko%2FM4YA%3D
%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd07c378b39c45-SIN
Alt-Svc: h3=":443"; ma=86400

<!DOCTYPE html><html lang=zh-CN><head><meta charset=utf-8><meta http-equiv=X-UA-Compatible content="IE=edge"><link rel="shortcut icon" type=image/x-icon
href=/static/icon.png?11><meta name=viewport co
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **history.replaceState.**

The following value was injected into the source:

```
https://okx2222.com/?p4iyoobk0n=p4iyoobk0n%27%22`'"/p4iyoobk0n/><p4iyoobk0n/\>rdoydb0g4e&#p4iyoobk0n=p4iyoobk0n%27%22`'"/p4iyoobk0n/><p4iyoobk0n/\>rdo
```

The previous value reached the sink as:

```
https://okx2222.com/?p4iyoobk0n=p4iyoobk0n%27%22`'"/p4iyoobk0n/><p4iyoobk0n/\>rdoydb0g4e&#/fw17e44419=fw17e44419'"`'"/fw17e44419/><fw17e44419/\>ej3wvn
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href (<anonymous>:1:323401)
at re (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149872)
at oe (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:150009)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149723)
at new e (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:148039)
at new se (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151248)
at i (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:185697)
at k (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:185770)
at l (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:90562)
at xr.beforeCreate (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:160806)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:11940)
at Dn (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:29997)
at t._init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:35336)
at new xr (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36144)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73458)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at t (https://okx2222.com/static/js/index.247330ad.js:1:431)
at https://okx2222.com/static/js/index.247330ad.js:1:8503
at https://okx2222.com/static/js/index.247330ad.js:1:8508
```

The stack trace at the sink was:

```
at Object.AdTdD (<anonymous>:1:618162)
at History.replaceState (<anonymous>:1:618402)
at Pt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142003)
at Mt (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:142146)
at oe (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:150006)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:149723)
at new e (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:148039)
at new se (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:151248)
at i (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:185697)
at k (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:185770)
at l (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:90562)
at xr.beforeCreate (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:29:160806)
at ee (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:11940)
at Dn (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:29997)
at t._init (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:35336)
at new xr (https://okx2222.com/static/js/chunk-vendors.a5da4e01.js:35:36144)
at 292d (https://okx2222.com/static/js/index.247330ad.js:1:73458)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at 0 (https://okx2222.com/static/js/index.247330ad.js:1:8538)
at d (https://okx2222.com/static/js/index.247330ad.js:1:6836)
at t (https://okx2222.com/static/js/index.247330ad.js:1:431)
at https://okx2222.com/static/js/index.247330ad.js:1:8503
at https://okx2222.com/static/js/index.247330ad.js:1:8508
```

---

4. Cacheable HTTPS response

There are 9 instances of this issue:

- /
- /api/chain/getOpenCurrencyList
- /api/common/getAppConfigAndCompanyConfig
- /api/common/getCustomerServiceConfig
- /api/common/getExplainList
- /api/common/getProductList
- /api/common/getSlide
- /api/common/pageNotice
- /static/js/pages-home-index.d13e0d47.js

Issue description

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-524: Information Exposure Through Caching
- CWE-525: Information Exposure Through Browser Caching
- CAPEC-37: Retrieve Embedded Sensitive Data

4.1. https://okx2222.com/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://okx2222.com**
Path:	**/**

Request

```
GET / HTTP/1.1
Host: okx2222.com
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/123.0.6312.122 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/2 200 OK
Date: Wed, 01 May 2024 04:29:24 GMT
Content-Type: text/html
Last-Modified: Fri, 26 Apr 2024 12:27:45 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=nuW71HmiieFuShjGTNBnBni%2BpzM9lOVfTeENNzgEvp4MgCcMVWSHUWzYCYOXo%2BcmIrBFEt4Rt8mjIloBRCI4PXI52SPfXfmP6Xf0SyaG15FzL9AZp1IzgIgko%2FM4YA%3D
%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd07c378b39c45-SIN
Alt-Svc: h3=":443"; ma=86400

<!DOCTYPE html><html lang=zh-CN><head><meta charset=utf-8><meta http-equiv=X-UA-Compatible content="IE=edge"><link rel="shortcut icon" type=image/x-icon
href=/static/icon.png?11><meta name=viewport co
...[SNIP]...
```

4.2. https://okx2222.com/api/chain/getOpenCurrencyList

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://okx2222.com**
Path:	**/api/chain/getOpenCurrencyList**

Request

```
POST /api/chain/getOpenCurrencyList HTTP/2
Host: okx2222.com
Accept-Encoding: gzip, deflate, br
Accept: */*
```

```
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://okx2222.com
uid: 0
Referer: https://okx2222.com/
x-requested-with: xmlhttprequest
content-type: application/json
accessToken:
sid: uR0xNsSbqSof3DwXa47Mo8ZT4TzMZ8d7
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: 24

KX2W79evbZU/ttgNOzbcFA==
```

Response

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 04:31:03 GMT
Content-Type: application/json
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=2gbvPD%2FLMg9RAvc1V7di53TVNN76qzrH55SiFGFNwgPKq07PwmS9gu%2Bp9Xasvt3MfAzXZegc20imTz9Hm4wHrLJIGe9pk%2B89mUqoCKvkPAA0SYuzYkC3Mw6FHwIWQA
%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd0a2e38e549ae-SIN
Alt-Svc: h3=":443"; ma=86400

"I1rQF5feJm/tITYfQISp4LxKCteUdvOx06FF+IUirWJ9sfLnDdifDWvR9SgOUeoHcpMbGdK5BfoyNZTHGa01r4G0RC17QfvL+y4TNNY0NgIqiwPpK7WbjBAx99DctCtv7+eubm2PWkOi3f
qEYdS8H6HW8mA1QKh1zST9LSQ+qUkiop5BPCcBx6gPHI/qySefpJjUpFJ
...[SNIP]...
```

4.3. https://okx2222.com/api/common/getAppConfigAndCompanyConfig

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://okx2222.com**
Path:	**/api/common/getAppConfigAndCompanyConfig**

Request

```
POST /api/common/getAppConfigAndCompanyConfig HTTP/2
Host: okx2222.com
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://okx2222.com
uid: 0
Referer: https://okx2222.com/
x-requested-with: xmlhttprequest
content-type: application/json
accessToken:
sid: uR0xNsSbqSof3DwXa47Mo8ZT4TzMZ8d7
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: 24

KX2W79evbZU/ttgNOzbcFA==
```

Response

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 04:30:34 GMT
Content-Type: application/json
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=X4pEDp%2FSiuOjhodhBPrqCxKw9DXs7xUJD5tBHX0Umr6xOWmAT0Tyk3xPJ%2F3Zpg9o7tVh%2B%2FGzIAlbzCUo18E36NQcxad21xGnMEev%2FaAB07x3YSdqDa4zDWd1NX
o5pQ%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd0978aa139d06-SIN
Alt-Svc: h3=":443"; ma=86400

"I1rQF5feJm/tITYfQISp4LxKCteUdvOx06FF+IUirWJ9sfLnDdifDWvR9SgOUeoHb46FNebLVFrAopFhwtOngCsNfpTXWiy46D+oE7EkiY/fsngJqqaLPDOuZLgCpgcr5puFNgjMPu4xDVlb
mmi0SpI+hI8wBnOI76HDBxTn7XQCd1Gw4nd1z1twx5kPLhEmGs9BMta
...[SNIP]...
```

4.4. https://okx2222.com/api/common/getCustomerServiceConfig

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://okx2222.com**

Path: **/api/common/getCustomerServiceConfig**

Request

```
POST /api/common/getCustomerServiceConfig HTTP/2
Host: okx2222.com
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://okx2222.com
uid: 0
Referer: https://okx2222.com/
x-requested-with: xmlhttprequest
content-type: application/json
accessToken:
sid: uR0xNsSbqSof3DwXa47Mo8ZT4TzMZ8d7
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: 24

KX2W79evbZU/ttgNOzbcFA==
```

Response

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 04:30:34 GMT
Content-Type: application/json
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=RapndUjTZFhUGb13j5avAniet%2Frv8fUdJ5E6auknMD0saLr80EhESipx9NKJhM9VeWGCNwfixgnIYIR0q8Ny%2BSL6z8jGbkX2v3QO2cH7drHGmRC37tGH3Vm5CTdTMA%3D%3
D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd0978aa0e9d06-SIN
Alt-Svc: h3=":443"; ma=86400

"I1rQF5feJm/tITYfQISp4LxKCteUdvOx06FF+IUirWJ9sfLnDdifDWvR9SgOUeoHRU46329YAavA42boGsDbZw=="
```

4.5. https://okx2222.com/api/common/getExplainList

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://okx2222.com**

Path: **/api/common/getExplainList**

Request

```
POST /api/common/getExplainList HTTP/2
Host: okx2222.com
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://okx2222.com
uid: 0
Referer: https://okx2222.com/
x-requested-with: xmlhttprequest
content-type: application/json
accessToken:
sid: uR0xNsSbqSof3DwXa47Mo8ZT4TzMZ8d7
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: 24

nfWvGKA8tSxBAOtHJkG6/A==
```

Response

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 04:31:03 GMT
Content-Type: application/json
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=GpgdLIpiH0r9uDbnqbfNE%2B0%2BOJ3ozHJAf4vdC3k%2BTUcda1UEwPHhHpNcGPBXIdOpw%2BsjjIAyT3zFInSI3wtjCI5hKPo1ML8cBDiZujROiE6NXfP798PU5IJrVYRkIQ%3D%3
```

```
D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd0a2e48f049ae-SIN
Alt-Svc: h3=":443"; ma=86400

"I1rQF5feJm/tlTYfQISp4LxKCteUdvOx06FF+IUirWJ9sfLnDdifDWvR9SgOUeoHbWeH1oiXzdb76/IG1IrvAJLQu91wP5GQyIhGgi3MS36wCru06zwhROXkgowjAYmmFMhwojeMCv3VC
UlPIfI+Z0NPOSAxKILjC+Gr2t4qpw7GvJG/VbQ3Eb519k/2T3cbjIBhneo
...[SNIP]...
```

4.6. https://okx2222.com/api/common/getProductList

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://okx2222.com**
Path:	**/api/common/getProductList**

Request

```
POST /api/common/getProductList HTTP/2
Host: okx2222.com
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://okx2222.com
uid: 0
Referer: https://okx2222.com/
x-requested-with: xmlhttprequest
content-type: application/json
accessToken:
sid: uR0xNsSbqSof3DwXa47Mo8ZT4TzMZ8d7
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: 24

KX2W79evbZU/ttgNOzbcFA==
```

Response

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 04:31:03 GMT
Content-Type: application/json
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vYqqNrDEibTaeLObwPzhANKqbTjgrbZJAuc286m%2FI%2Fhmn2LbCoVnw2gEBp%2BQHTBBOUAbFkIAfkfdr7zPNhwRMmJMZabIt2ssA%2FuaAAq8I2NNQLKH6JELJPGQeEFMe
g%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd0a2e38e649ae-SIN
Alt-Svc: h3=":443"; ma=86400

"I1rQF5feJm/tlTYfQISp4LxKCteUdvOx06FF+IUirWJ9sfLnDdifDWvR9SgOUeoHRU46329YAavA42boGsDbZw=="
```

4.7. https://okx2222.com/api/common/getSlide

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://okx2222.com**
Path:	**/api/common/getSlide**

Request

```
POST /api/common/getSlide HTTP/2
Host: okx2222.com
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://okx2222.com
uid: 0
Referer: https://okx2222.com/
x-requested-with: xmlhttprequest
content-type: application/json
accessToken:
sid: uR0xNsSbqSof3DwXa47Mo8ZT4TzMZ8d7
```

```
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: 24

uQ/0gw9tSSsTMmoFarufdQ==
```

Response


```
HTTP/2 200 OK
Date: Wed, 01 May 2024 04:31:03 GMT
Content-Type: application/json
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=dXVfOrIKRfAMwPWqqOoHCJsrDjoJ04rnTCPheXvduEwbgVC8FP4s3xKVyCBEJ3fkw33P9G4t0FLGkqTmZRb1rWmCfWIBv0IRU0DVEQVz3HAefx0NO9JLQYScAlr5MA%3D%3D"}]
,"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd0a2e48ec49ae-SIN
Alt-Svc: h3=":443"; ma=86400

"I1rQF5feJm/tlTYfQISp4LxKCteUdvOx06FF+IUirWJ9sfLnDdifDWvR9SgOUeoHrZOLscSEjf1DLQPckDbm7MkgpKwh326YVvVLyS5DdgkAkwUyxIGG8UDa3ZltNRJ+VgVoCdB1Iq5waQ
H3jN3EHz6hhLvEBViT+zi43o6n009OTxBNSkbI1XD02TbZVS5yGlNMeLO
...[SNIP]...
```

4.8. https://okx2222.com/api/common/pageNotice

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://okx2222.com**
Path:	**/api/common/pageNotice**

Request

```
POST /api/common/pageNotice HTTP/2
Host: okx2222.com
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://okx2222.com
uid: 0
Referer: https://okx2222.com/
x-requested-with: xmlhttprequest
content-type: application/json
accessToken:
sid: uR0xNsSbqSof3DwXa47Mo8ZT4TzMZ8d7
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: 88

zqvg/TlKf5e6ON7K1sV+nR6sd+UwHtYYxDxQopaOjvbalWTApKM7JgwE3vXX6DQF2tse89NVuTWN4gF35yLsiw==
```

Response


```
HTTP/2 200 OK
Date: Wed, 01 May 2024 04:31:03 GMT
Content-Type: application/json
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=cFLT1cY6xyaSAPSfQoxGni%2FOZRhBgQ9AcR82rmfobpmOnkwQvYm7cdNXIgregygRKj0ZPtcTFtcQ0uESJFnJM9tFtS9ndJfJWvf2tfxSMi00DHDVwi1Vo3fS%2FuVjZQ%3D%3D"}],
"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd0a2e38e449ae-SIN
Alt-Svc: h3=":443"; ma=86400

"I1rQF5feJm/tlTYfQISp4LxKCteUdvOx06FF+IUirWJ9sfLnDdifDWvR9SgOUeoHShImjchqGHjjeISdEGMIneOGQeFcAnWxqpOi/dB2GzBQSm/xLKRjrQI0mWFxCCs0iYUqB8w/tqvBWf21
DIjBIyDCDttyIGgNagIdd0R3XioJtmSg82uAsINKEyG+36w096q5Ytp
...[SNIP]...
```

4.9. https://okx2222.com/static/js/pages-home-index.d13e0d47.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://okx2222.com**
Path:	**/static/js/pages-home-index.d13e0d47.js**

Request

```
GET /static/js/pages-home-index.d13e0d47.js HTTP/2
Host: okx2222.com
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/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://okx2222.com/
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/2 200 OK
Date: Wed, 01 May 2024 04:30:43 GMT
Content-Type: application/javascript
Last-Modified: Fri, 26 Apr 2024 12:29:00 GMT
Vary: Accept-Encoding
Etag: W/"662b9e0c-c1c0"
Expires: Wed, 01 May 2024 07:54:37 GMT
Cache-Control: max-age=14400
Cf-Cache-Status: HIT
Age: 2166
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=NbvxET27znjVFKEGf70uE1aqF%2BZQpXxoDyz1fhMX8weXBPA7k9bxxZYdr0OHaov3DZ31sfJidRmeXIt76vsBUn7hYWDuc49CCTdnA3yg1tjT93iJlaZySnHIh3mg6Q%3D%3D"}],"gr
oup":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 87cd09afae629d06-SIN
Alt-Svc: h3=":443"; ma=86400

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["pages-home-index"],{"00a0":function(t,e,n){"use strict";n("a9e3"),Object.defineProperty(e,"__esModule",
{value:!0}),e.default=void 0;var i={p
...[SNIP]...
```

---

5. TLS certificate

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://okx2222.com**
Path:	**/**

Issue detail

The server presented a valid, trusted TLS certificate. This issue is purely informational.

The server presented the following certificates:

Server certificate

Issued to:	okx2222.com, *.okx2222.com
Issued by:	GTS CA 1P5
Valid from:	Wed Mar 20 19:21:36 IST 2024
Valid to:	Tue Jun 18 19:21:35 IST 2024

Certificate chain #1

Issued to:	GTS CA 1P5
Issued by:	GTS Root R1
Valid from:	Thu Aug 13 05:30:42 IST 2020
Valid to:	Thu Sep 30 05:30:42 IST 2027

Certificate chain #2

Issued to:	GTS Root R1
Issued by:	GlobalSign Root CA
Valid from:	Fri Jun 19 05:30:42 IST 2020
Valid to:	Fri Jan 28 05:30:42 IST 2028

Certificate chain #3

Issued to:	GlobalSign Root CA
Issued by:	GlobalSign Root CA
Valid from:	Tue Sep 01 17:30:00 IST 1998
Valid to:	Fri Jan 28 17:30:00 IST 2028

Issue background

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

References

- SSL/TLS Configuration Guide

Vulnerability classifications

- CWE-295: Improper Certificate Validation
- CWE-326: Inadequate Encryption Strength
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm