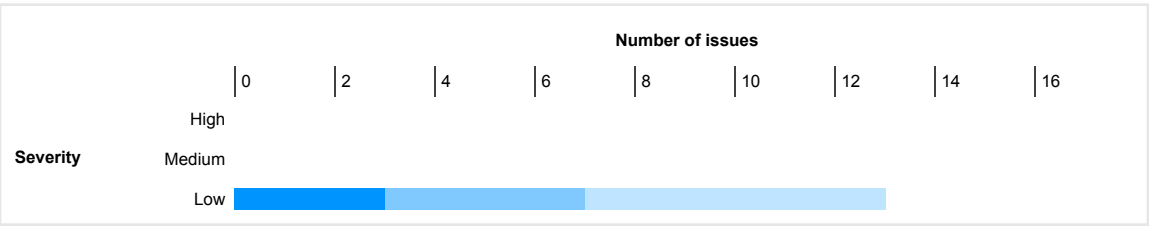
Burp Scanner Report

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	3	4	6	13
	Information	7	11	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. Client-side JSON injection (DOM-based)

There are 2 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-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. https://www.ourshopee.com/

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://www.ourshopee.com**
Path:	**/**

Issue detail

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

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2CddGOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **postMessage** and passed to **JSON.parse**.

The application passed a string to the event handler with value:

```
__ym__promise_5668393_1061028596
```

The following value was injected into the event handler and reached the sink without any modification:

```
pt0jk8mt4b%2527%2522`'"/pt0jk8mt4b/><pt0jk8mt4b/\>elchk1gpk7&__ym__promise_5668393_1061028596
```

The stack trace at the source was:

```
at _0x576d9d (<anonymous>:1:418076)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at Object.lfqNk (<anonymous>:1:104147)
at Object.AWngC (<anonymous>:1:438456)
at _0x3fd616.<computed> (<anonymous>:1:463194)
at https://sc-static.net/scevent.min.js:2:49291
at https://sc-static.net/scevent.min.js:2:4779
at m (https://sc-static.net/scevent.min.js:2:2806)
at s (https://sc-static.net/scevent.min.js:2:4756)
at m (https://sc-static.net/scevent.min.js:2:2806)
at Y.c.send (https://sc-static.net/scevent.min.js:2:5064)
at https://sc-static.net/scevent.min.js:2:6916
at m (https://sc-static.net/scevent.min.js:2:2806)
at c (https://sc-static.net/scevent.min.js:2:6893)
at Object.HSSaF (<anonymous>:1:409571)
at _0x576d9d (<anonymous>:1:419059)
```

The stack trace at the event listener was:

```
at Object.BQODu (<anonymous>:1:95774)
at Object.pLXLD (<anonymous>:1:395292)
at Object.UyhhO (<anonymous>:1:404582)
at <anonymous>:1:409830
at https://sc-static.net/scevent.min.js:2:6981
at m (https://sc-static.net/scevent.min.js:2:2806)
at Mt (https://sc-static.net/scevent.min.js:2:6842)
at https://sc-static.net/scevent.min.js:2:49250
at https://sc-static.net/scevent.min.js:2:4779
at m (https://sc-static.net/scevent.min.js:2:2806)
at s (https://sc-static.net/scevent.min.js:2:4756)
at c (https://sc-static.net/scevent.min.js:2:4856)
at https://sc-static.net/scevent.min.js:2:49235
at https://sc-static.net/scevent.min.js:2:50666
```

The event listener that receives the message does not validate the origin.

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

The origin used in the proof of concept was:

```
https://www.ourshopee.com.fakeourshopee.com
```

The following proof of concept was generated for this issue:

```
<script>
function poc(){
window.win=window.open('https://www.ourshopee.com/');
var msg='//__ym__promise_5668393_1061028596';
setTimeout(function(){win.postMessage(msg,'*');}, 5000);
}
</script>
<a href="#" onclick="poc();">PoC</a>
```

1.2. https://www.ourshopee.com/

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://www.ourshopee.com**
Path:	**/**

Issue detail

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

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2CddGOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **postMessage** and passed to **JSON.parse**.

The application passed a string to the event handler with value:

```
__ym__promise_5668393_1061028596
```

The following value was injected into the event handler and reached the sink without any modification:

```
iksbdinzdb%2527%2522`'"/iksbdinzdb/><iksbdinzdb/\>n904rsab1q&__ym__promise_5668393_1061028596
```

The stack trace at the source was:

```
at _0x576d9d (<anonymous>:1:418076)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at Object.lfqNk (<anonymous>:1:104147)
at Object.AWngC (<anonymous>:1:438456)
at _0x3fd616.<computed> (<anonymous>:1:463194)
at Jb (https://mc.yandex.ru/metrika/tag.js:168:357)
at https://mc.yandex.ru/metrika/tag.js:218:20
at https://mc.yandex.ru/metrika/tag.js:145:407
at https://mc.yandex.ru/metrika/tag.js:145:316
at Object.HSSaF (<anonymous>:1:409571)
at _0x576d9d (<anonymous>:1:419059)
```

The stack trace at the event listener was:

```
at Object.BQODu (<anonymous>:1:95774)
at Object.pLXLD (<anonymous>:1:395292)
at Object.UyhhO (<anonymous>:1:404582)
```

```
at <anonymous>:1:409830
at Qj (https://mc.yandex.ru/metrika/tag.js:145:208)
at https://mc.yandex.ru/metrika/tag.js:209:206
at Array.map (<anonymous>)
at Jk (https://mc.yandex.ru/metrika/tag.js:194:325)
at Object.F (https://mc.yandex.ru/metrika/tag.js:209:181)
at https://mc.yandex.ru/metrika/tag.js:220:36
at https://mc.yandex.ru/metrika/tag.js:158:241
at $i (https://mc.yandex.ru/metrika/tag.js:100:270)
at https://mc.yandex.ru/metrika/tag.js:231:61
at https://mc.yandex.ru/metrika/tag.js:145:407
at https://mc.yandex.ru/metrika/tag.js:145:316
at https://mc.yandex.ru/metrika/tag.js:91:221
at f (https://mc.yandex.ru/metrika/tag.js:1:123)
at Array.map (<anonymous>)
at Jk (https://mc.yandex.ru/metrika/tag.js:194:325)
at https://mc.yandex.ru/metrika/tag.js:2:196
at https://mc.yandex.ru/metrika/tag.js:145:407
at new $e (https://mc.yandex.ru/metrika/tag.js:2:204)
at https://mc.yandex.ru/metrika/tag.js:401:128
at https://mc.yandex.ru/metrika/tag.js:161:496
at ua (https://mc.yandex.ru/metrika/tag.js:159:109)
at https://mc.yandex.ru/metrika/tag.js:161:427
at Array.map (<anonymous>)
at Jk (https://mc.yandex.ru/metrika/tag.js:194:325)
at https://mc.yandex.ru/metrika/tag.js:161:427
at gk (https://mc.yandex.ru/metrika/tag.js:162:25)
```

The event listener that receives the message does not validate the origin.

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

The origin used in the proof of concept was:

```
https://www.ourshopee.com.fakeourshopee.com
```

The following proof of concept was generated for this issue:

```
<script>
function poc(){
window.win=window.open('https://www.ourshopee.com/');
var msg='//__ym__promise_5668393_1061028596';
setTimeout(function(){win.postMessage(msg,'*');}, 5000);
}
</script>
<a href="#" onclick="poc();">PoC</a>
```

---

2. Open redirection (DOM-based)

There are 6 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-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. https://www.ourshopee.com/

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://www.ourshopee.com**
Path:	**/**

Issue detail

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

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2CddGOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

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

The following value was injected into the source:

```
/////pgyyj1lgns%27%22%60'%22/pgyyj1lgns/%3E%3Cpgyyj1lgns//%3Ez7fcnhywp8&
```

The previous value reached the sink as:

```
{"memory":{"totalJSHeapSize":56800000,"usedJSHeapSize":47400000,"jsHeapSizeLimit":2190000000},"resources":[],"referrer":"https://www.ourshope
```

The stack trace at the source was:

```
at Object._0x165f99 [as proxiedGetterCallback] (<anonymous>:1:557377)
at get pathname (<anonymous>:1:249642)
at e (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:1745)
at https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:3321
at P (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:4083)
at R (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:5055)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.<computed>._0x13cc4d.oknbI._0x3e2633.XMLHttpRequest.<computed> (<anonymous>:1:458938)
at XMLHttpRequest.send (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:171137)
at t.sendObjectBeacon (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:9090)
at P (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:4135)
at R (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:5055)
```

2.2. https://www.ourshopee.com/

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://www.ourshopee.com**
Path:	**/**

Issue detail

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

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2Cdd
GOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

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

The following value was injected into the source:

```
https://www.ourshopee.com/?pgmjcd3r0r=pgmjcd3r0r%27%22%60'%22/pgmjcd3r0r/%3E%3Cpgmjcd3r0r/\%3Elwww87vhm9&
```

The previous value reached the sink as:

```
{"memory":{"totalJSHeapSize":56800000,"usedJSHeapSize":47400000,"jsHeapSizeLimit":2190000000},"resources":[],"referrer":"https://www.ourshope
```

The stack trace at the source was:

```
at HTMLDocument.get [as referrer] (<anonymous>:1:276163)
at https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:3383
at P (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:4083)
at R (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:5055)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.<computed>._0x13cc4d.oknbI._0x3e2633.XMLHttpRequest.<computed> (<anonymous>:1:458938)
at XMLHttpRequest.send (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:171137)
at t.sendObjectBeacon (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:9090)
at P (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:4135)
at R (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:5055)
```

The following proof of concept was generated for this issue:

```
<!-- Visit from your domain -->
http://your-domain?
```

```
<!-- Link back to site from your domain -->
<a href="https://www.ourshopee.com/">PoC</a>
```

2.3. https://www.ourshopee.com/

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://www.ourshopee.com**
Path:	**/**

Issue detail

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

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2CddGOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet" media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

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

The following value was injected into the source:

```
/////ueujq8kk5o%27%22%60'%22/ueujq8kk5o/%3E%3Cueujq8kk5o//%3Exmtabpspkt&
```

The previous value reached the sink as:

```
{"resources":[],"referrer":"https://www.ourshopee.com/?t7rfr8csnq=t7rfr8csnq%27%22%60'%22/t7rfr8csnq/%3E%3Ct7rfr8csnq/\\%3Elpmygk5zf9&","even
```

The stack trace at the source was:

```
at Object._0x165f99 [as proxiedGetterCallback] (<anonymous>:1:557377)
at get pathname (<anonymous>:1:249642)
at e (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:1745)
at t.pushState (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:5498)
at b.<computed> (https://connect.facebook.net/en_US/fbevents.js:24:49796)
at c.<computed> (https://www.googletagmanager.com/gtag/js?id=G-VSQBESP2WG&l=dataLayer&cx=c:591:250)
at history.pushState (https://www.clarity.ms/s/0.7.32/clarity.js:2:57026)
at History.<anonymous> (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:317500)
at History.pushState (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:266896)
at push (https://www.ourshopee.com/static/js/main.6eee6505.js:1:481445)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:489828
at onClick (https://www.ourshopee.com/static/js/main.6eee6505.js:1:545268)
at Object.De (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169751)
at Ue (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169905)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:189805
at Rr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:189899)
at Fr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:190314)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:195756
```

```
at uc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:259468)
at Te (https://www.ourshopee.com/static/js/main.6eee6505.js:1:168883)
at Wr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:191608)
at Gt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:176004)
at Yt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:175788)
at _0x14405e (<anonymous>:1:147957)
at _0x2a880c (<anonymous>:1:151903)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.<computed>._0x13cc4d.oknbI._0x3e2633.XMLHttpRequest.<computed> (<anonymous>:1:458938)
at XMLHttpRequest.send (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:171137)
at t.sendObjectBeacon (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:9090)
at P (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:4135)
at t.pushState (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:5594)
at b.<computed> (https://connect.facebook.net/en_US/fbevents.js:24:49796)
at c.<computed> (https://www.googletagmanager.com/gtag/js?id=G-VSQBESP2WG&l=dataLayer&cx=c:591:250)
at history.pushState (https://www.clarity.ms/s/0.7.32/clarity.js:2:57026)
at History.<anonymous> (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:317500)
at History.pushState (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:266896)
at push (https://www.ourshopee.com/static/js/main.6eee6505.js:1:481445)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:489828
at onClick (https://www.ourshopee.com/static/js/main.6eee6505.js:1:545268)
at Object.De (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169751)
at Ue (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169905)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:189805
at Rr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:189899)
at Fr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:190314)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:195756
at uc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:259468)
at Te (https://www.ourshopee.com/static/js/main.6eee6505.js:1:168883)
at Wr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:191608)
at Gt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:176004)
at Yt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:175788)
at _0x14405e (<anonymous>:1:147957)
at _0x2a880c (<anonymous>:1:151903)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

This was triggered by a **click** event with the following HTML:

```
<li class="breadcrumb-item Homepage"><a href="#" role="button" tabindex="0"> Home </a></li>
```

2.4. https://www.ourshopee.com/

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://www.ourshopee.com**
Path:	**/**

Issue detail

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

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2Cdd
```

GOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet" media="screen" href="https:/
...[SNIP]...

Dynamic analysis

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

The following value was injected into the source:

```
https://www.ourshopee.com/?t7rfr8csnq=t7rfr8csnq%27%22%60'%22/t7rfr8csnq/%3E%3Ct7rfr8csnq/\%3Elpmygk5zf9&
```

The previous value reached the sink as:

```
{"resources":[],"referrer":"https://www.ourshopee.com/?t7rfr8csnq=t7rfr8csnq%27%22%60'%22/t7rfr8csnq/%3E%3Ct7rfr8csnq/\\%3Elpmygk5zf9&","even
```

The stack trace at the source was:

```
at HTMLDocument.get [as referrer] (<anonymous>:1:276163)
at https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:3383
at P (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:4083)
at t.pushState (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:5594)
at b.<computed> (https://connect.facebook.net/en_US/fbevents.js:24:49796)
at c.<computed> (https://www.googletagmanager.com/gtag/js?id=G-VSQBESP2WG&l=dataLayer&cx=c:591:250)
at history.pushState (https://www.clarity.ms/s/0.7.32/clarity.js:2:57026)
at History.<anonymous> (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:317500)
at History.pushState (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:266896)
at push (https://www.ourshopee.com/static/js/main.6eee6505.js:1:481445)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:489828
at onClick (https://www.ourshopee.com/static/js/main.6eee6505.js:1:545268)
at Object.De (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169751)
at Ue (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169905)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:189805
at Rr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:189899)
at Fr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:190314)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:195756
at uc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:259468)
at Te (https://www.ourshopee.com/static/js/main.6eee6505.js:1:168883)
at Wr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:191608)
at Gt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:176004)
at Yt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:175788)
at _0x14405e (<anonymous>:1:147957)
at _0x2a880c (<anonymous>:1:151903)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.<computed>._0x13cc4d.oknbI._0x3e2633.XMLHttpRequest.<computed> (<anonymous>:1:458938)
at XMLHttpRequest.send (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:171137)
at t.sendObjectBeacon (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:9090)
at P (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:4135)
at t.pushState (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:5594)
at b.<computed> (https://connect.facebook.net/en_US/fbevents.js:24:49796)
at c.<computed> (https://www.googletagmanager.com/gtag/js?id=G-VSQBESP2WG&l=dataLayer&cx=c:591:250)
at history.pushState (https://www.clarity.ms/s/0.7.32/clarity.js:2:57026)
at History.<anonymous> (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:317500)
at History.pushState (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:266896)
at push (https://www.ourshopee.com/static/js/main.6eee6505.js:1:481445)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:489828
at onClick (https://www.ourshopee.com/static/js/main.6eee6505.js:1:545268)
at Object.De (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169751)
at Ue (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169905)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:189805
at Rr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:189899)
at Fr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:190314)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:195756
at uc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:259468)
at Te (https://www.ourshopee.com/static/js/main.6eee6505.js:1:168883)
at Wr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:191608)
at Gt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:176004)
at Yt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:175788)
at _0x14405e (<anonymous>:1:147957)
at _0x2a880c (<anonymous>:1:151903)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

This was triggered by a **click** event with the following HTML:

```
<li class="breadcrumb-item Homepage"><a href="#" role="button" tabindex="0"> Home </a></li>
```

The following proof of concept was generated for this issue:

```
<!-- Visit from your domain -->
http://your-domain?
```

```
<!-- Link back to site from your domain -->
<a href="https://www.ourshopee.com/">PoC</a>
```

2.5. https://www.ourshopee.com/

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://www.ourshopee.com**
Path:	**/**

Issue detail

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

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2CddGOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

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

The following value was injected into the source:

```
/////b8qmjsq5j3%27%22%60'%22/b8qmjsq5j3/%3E%3Cb8qmjsq5j3//%3Exxnhxmg4xm&
```

The previous value reached the sink as:

```
{"resources":[],"referrer":"https://www.ourshopee.com/?famh47rve7=famh47rve7%27%22%60'%22/famh47rve7/%3E%3Cfamh47rve7/\\%3Ebl0vkeeg1h&","even
```

The stack trace at the source was:

```
at Object._0x165f99 [as proxiedGetterCallback] (<anonymous>:1:557377)
at get pathname (<anonymous>:1:249642)
at e (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:1745)
at t.pushState (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:5498)
at b.<computed> (https://connect.facebook.net/en_US/fbevents.js:24:49796)
at c.<computed> (https://www.googletagmanager.com/gtag/js?id=G-VSQBESP2WG&l=dataLayer&cx=c:591:250)
at History.<anonymous> (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:317500)
at History.<anonymous> (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:266896)
at history.pushState (https://www.clarity.ms/s/0.7.32/clarity.js:2:57026)
at push (https://www.ourshopee.com/static/js/main.6eee6505.js:1:481445)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:489828
at onClick (https://www.ourshopee.com/static/js/main.6eee6505.js:1:545268)
at Object.De (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169751)
at Ue (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169905)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:189805
at Rr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:189899)
at Fr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:190314)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:195756
```

```
at uc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:259468)
at Te (https://www.ourshopee.com/static/js/main.6eee6505.js:1:168883)
at Wr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:191608)
at Gt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:176004)
at Yt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:175788)
at _0x14405e (<anonymous>:1:147957)
at _0x2a880c (<anonymous>:1:151903)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.<computed>._0x13cc4d.oknbI._0x3e2633.XMLHttpRequest.<computed> (<anonymous>:1:458938)
at XMLHttpRequest.send (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:171137)
at t.sendObjectBeacon (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:9090)
at P (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:4135)
at t.pushState (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:5594)
at b.<computed> (https://connect.facebook.net/en_US/fbevents.js:24:49796)
at c.<computed> (https://www.googletagmanager.com/gtag/js?id=G-VSQBESP2WG&l=dataLayer&cx=c:591:250)
at History.<anonymous> (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:317500)
at History.<anonymous> (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:266896)
at history.pushState (https://www.clarity.ms/s/0.7.32/clarity.js:2:57026)
at push (https://www.ourshopee.com/static/js/main.6eee6505.js:1:481445)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:489828
at onClick (https://www.ourshopee.com/static/js/main.6eee6505.js:1:545268)
at Object.De (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169751)
at Ue (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169905)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:189805
at Rr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:189899)
at Fr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:190314)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:195756
at uc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:259468)
at Te (https://www.ourshopee.com/static/js/main.6eee6505.js:1:168883)
at Wr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:191608)
at Gt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:176004)
at Yt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:175788)
at _0x14405e (<anonymous>:1:147957)
at _0x2a880c (<anonymous>:1:151903)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

This was triggered by a **click** event with the following HTML:

```
<li class="breadcrumb-item Homepage"><a href="#" role="button" tabindex="0"> Home </a></li>
```

2.6. https://www.ourshopee.com/

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://www.ourshopee.com**
Path:	**/**

Issue detail

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

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2Cdd
```

```
GOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

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

The following value was injected into the source:

```
https://www.ourshopee.com/?famh47rve7=famh47rve7%27%22%60'%22/famh47rve7/%3E%3Cfamh47rve7/\%3Ebl0vkeeg1h&
```

The previous value reached the sink as:

```
{"resources":[],"referrer":"https://www.ourshopee.com/?famh47rve7=famh47rve7%27%22%60'%22/famh47rve7/%3E%3Cfamh47rve7/\\%3Ebl0vkeeg1h&","even
```

The stack trace at the source was:

```
at HTMLDocument.get [as referrer] (<anonymous>:1:276163)
at https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:3383
at P (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:4083)
at t.pushState (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:5594)
at b.<computed> (https://connect.facebook.net/en_US/fbevents.js:24:49796)
at c.<computed> (https://www.googletagmanager.com/gtag/js?id=G-VSQBESP2WG&l=dataLayer&cx=c:591:250)
at History.<anonymous> (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:317500)
at History.<anonymous> (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:266896)
at history.pushState (https://www.clarity.ms/s/0.7.32/clarity.js:2:57026)
at push (https://www.ourshopee.com/static/js/main.6eee6505.js:1:481445)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:489828
at onClick (https://www.ourshopee.com/static/js/main.6eee6505.js:1:545268)
at Object.De (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169751)
at Ue (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169905)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:189805
at Rr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:189899)
at Fr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:190314)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:195756
at uc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:259468)
at Te (https://www.ourshopee.com/static/js/main.6eee6505.js:1:168883)
at Wr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:191608)
at Gt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:176004)
at Yt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:175788)
at _0x14405e (<anonymous>:1:147957)
at _0x2a880c (<anonymous>:1:151903)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.<computed>._0x13cc4d.oknbI._0x3e2633.XMLHttpRequest.<computed> (<anonymous>:1:458938)
at XMLHttpRequest.send (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:171137)
at t.sendObjectBeacon (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:9090)
at P (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:4135)
at t.pushState (https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015:1:5594)
at b.<computed> (https://connect.facebook.net/en_US/fbevents.js:24:49796)
at c.<computed> (https://www.googletagmanager.com/gtag/js?id=G-VSQBESP2WG&l=dataLayer&cx=c:591:250)
at History.<anonymous> (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:317500)
at History.<anonymous> (https://analytics.tiktok.com/i18n/pixel/static/main.MWU2NDEzYzJiMQ.js:2:266896)
at history.pushState (https://www.clarity.ms/s/0.7.32/clarity.js:2:57026)
at push (https://www.ourshopee.com/static/js/main.6eee6505.js:1:481445)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:489828
at onClick (https://www.ourshopee.com/static/js/main.6eee6505.js:1:545268)
at Object.De (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169751)
at Ue (https://www.ourshopee.com/static/js/main.6eee6505.js:1:169905)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:189805
at Rr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:189899)
at Fr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:190314)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:195756
at uc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:259468)
at Te (https://www.ourshopee.com/static/js/main.6eee6505.js:1:168883)
at Wr (https://www.ourshopee.com/static/js/main.6eee6505.js:1:191608)
at Gt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:176004)
at Yt (https://www.ourshopee.com/static/js/main.6eee6505.js:1:175788)
at _0x14405e (<anonymous>:1:147957)
at _0x2a880c (<anonymous>:1:151903)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

This was triggered by a **click** event with the following HTML:

```
<li class="breadcrumb-item Homepage"><a href="#" role="button" tabindex="0"> Home </a></li>
```

The following proof of concept was generated for this issue:

```
<!-- Visit from your domain -->
http://your-domain?
```

```
<!-- Link back to site from your domain -->
<a href="https://www.ourshopee.com/">PoC</a>
```

---

3. Link manipulation (DOM-based)

There are 2 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-based link manipulation arises when a script writes controllable data to a navigation target within the current page, such as a clickable link or the submission URL of a form. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the target of links within the response. An attacker may be able to leverage this to perform various attacks, including:

- Causing the user to redirect to an arbitrary external URL, to facilitate a phishing attack.
- Causing the user to submit sensitive form data to a server controlled by the attacker.
- Causing the user to perform an unintended action within the application, by changing the file or query string associated with a link.
- Bypassing browser anti-XSS defenses by injecting on-site links containing XSS exploits, since browser anti-XSS defenses typically do not operate on on-site links.

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 link manipulation vulnerabilities is not to dynamically set the target URLs of links or forms 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 link target. In general, this is best achieved by using a whitelist of URLs that are permitted link targets, and strictly validating the target against this list before setting the link target.

References

- Web Security Academy: Link manipulation (DOM-based)

Vulnerability classifications

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

3.1. https://www.ourshopee.com/

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://www.ourshopee.com**
Path:	**/**

Issue detail

The application may be vulnerable to DOM-based link manipulation. Data is read from **input.value** and passed to **element.setAttribute.href**.

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
```

```
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2CddGOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **element.setAttribute.href**.

The previous value reached the sink as:

```
/search-result/t99bw9rifl%2527%2522`'"/t99bw9rifl/><t99bw9rifl/\>k22z1s9gqs&
```

The stack trace at the source was:

```
at Object.BQODu (<anonymous>:1:95774)
at Object.USBMk (<anonymous>:1:394438)
at HTMLInputElement.get (<anonymous>:1:398284)
at HTMLInputElement.get [as value] (<anonymous>:1:514193)
at HTMLInputElement.get [as value] (https://www.ourshopee.com/static/js/main.6eee6505.js:1:162490)
at RS (https://www.ourshopee.com/static/js/main.6eee6505.js:1:1031366)
at Sa (https://www.ourshopee.com/static/js/main.6eee6505.js:1:216069)
at Es (https://www.ourshopee.com/static/js/main.6eee6505.js:1:227757)
at Sl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:274065)
at xc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:262288)
at yc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:262216)
at vc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:262079)
at oc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:257183)
at j (https://www.ourshopee.com/static/js/main.6eee6505.js:1:387981)
at MessagePort.P (https://www.ourshopee.com/static/js/main.6eee6505.js:1:388515)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at Object.fvZqN (<anonymous>:1:102549)
at _0x584248 (<anonymous>:1:483704)
at Object.dviwz (<anonymous>:1:103090)
at Object.WcOpF (<anonymous>:1:441942)
at Object.TrNlW (<anonymous>:1:485864)
at _0xdc6a5f.aQIHE._0xf9f2ea [as setAttribute] (<anonymous>:1:487694)
at b (https://www.ourshopee.com/static/js/main.6eee6505.js:1:156500)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:250633)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249978)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249978)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:250175)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:250175)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249978)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:250175)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:250175)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249978)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:250175)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249978)
```

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

3.2. https://www.ourshopee.com/

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://www.ourshopee.com**
Path:	**/**

Issue detail

The application may be vulnerable to DOM-based link manipulation. Data is read from **input.value** and passed to **element.setAttribute.href**.

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2CddGOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **element.setAttribute.href**.

The previous value reached the sink as:

```
/search-result/yhp7b163ks%2527%2522`'"/yhp7b163ks/><yhp7b163ks/\>w32brt1myf&
```

The stack trace at the source was:

```
at Object.BQODu (<anonymous>:1:95774)
at Object.USBMk (<anonymous>:1:394438)
at HTMLInputElement.get (<anonymous>:1:398284)
at HTMLInputElement.get [as value] (<anonymous>:1:514193)
at HTMLInputElement.get [as value] (https://www.ourshopee.com/static/js/main.6eee6505.js:1:162490)
at RS (https://www.ourshopee.com/static/js/main.6eee6505.js:1:1031366)
at Sa (https://www.ourshopee.com/static/js/main.6eee6505.js:1:216069)
at Es (https://www.ourshopee.com/static/js/main.6eee6505.js:1:227757)
at Sl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:274065)
at xc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:262288)
at yc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:262216)
at vc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:262079)
at cc (https://www.ourshopee.com/static/js/main.6eee6505.js:1:259195)
at Vi (https://www.ourshopee.com/static/js/main.6eee6505.js:1:199790)
at https://www.ourshopee.com/static/js/main.6eee6505.js:1:256792
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at Object.fvZqN (<anonymous>:1:102549)
at _0x584248 (<anonymous>:1:483704)
at Object.dviwz (<anonymous>:1:103090)
at Object.WcOpF (<anonymous>:1:441942)
at Object.TrNlW (<anonymous>:1:485864)
at _0xdc6a5f.aQIHE._0xf9f2ea [as setAttribute] (<anonymous>:1:487694)
at b (https://www.ourshopee.com/static/js/main.6eee6505.js:1:156500)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:250633)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249978)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249978)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:250175)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:250175)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249978)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:250175)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:250175)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249978)
```

```
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:250175)
at gl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249865)
at vl (https://www.ourshopee.com/static/js/main.6eee6505.js:1:249978)
```

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

---

4. Strict transport security not enforced

There are 3 instances of this issue:

- /
- /locales/en/translation.json
- /robots.txt

Issue description

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

4.1. https://www.ourshopee.com/

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://www.ourshopee.com**
Path:	**/**

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
```

```
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2CddGOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet" media="screen" href="https:/
...[SNIP]...
```

4.2. https://www.ourshopee.com/locales/en/translation.json

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://www.ourshopee.com**
Path:	**/locales/en/translation.json**

Request

```
GET /locales/en/translation.json HTTP/2
Host: www.ourshopee.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/126.0.6478.127 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://www.ourshopee.com/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:07:25 GMT
Content-Type: application/json
Last-Modified: Tue, 07 May 2024 09:55:57 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:07:25 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=osoTdhZKF%2BgTE0RfERvYR73Hi8etd1q%2BaKBq0Q%2B%2FcclPRHWx%2BZ97WfFTwLY%2FcLoNOf143pBnUQQu%2BP2Vddw6vLPLtLMEOAfXCSeKpdOfuLMKFAiE%2BmdqkgGE4%2By81%2BUqbSDW"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff4467af8e40a5-BOM
Alt-Svc: h3=":443"; ma=86400

{
"localization_testing": "ENGLISH",
"global.viewAll": "View All",
"global.addCart": "ADD TO CART",
"global.off": "OFF",

"home.excitingTitle": "Exciting Offers",
"home.
...[SNIP]...
```

4.3. https://www.ourshopee.com/robots.txt

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://www.ourshopee.com**
Path:	**/robots.txt**

Request

```
GET /robots.txt HTTP/2
Host: www.ourshopee.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/126.0.6478.127 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:18 GMT
Content-Type: text/plain
Last-Modified: Thu, 02 May 2024 10:39:54 GMT
Cache-Control: max-age=31536000
Expires: Thu, 25 Jul 2024 17:54:35 GMT
Cf-Cache-Status: HIT
Age: 804873
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=xkK3EqKYRJHQ8Uj8Re78w1Y%2BxuE1g38QfL04DqJCqsv0%2BCeSkVY4sn5tOmvBxTQ4ljnSK2AqZgcmVQuuqLNN0mLPv0KZRdZpbBfsunPeCG9O8mFQ7tLYpx1Fpg%2Bad7rMQyg
7"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Vary: Accept-Encoding
Server: cloudflare
Cf-Ray: 89ff414c1ee13e40-BOM
Alt-Svc: h3=":443"; ma=86400

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

---

5. Cross-domain script include

Summary

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

Issue detail

The response dynamically includes the following scripts from other domains:

- https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015
- https://www.googletagmanager.com/ns.html?id=GTM-MJN7RD8

Issue background

When an application includes a script from an external domain, this script is executed by the browser within the security context of the invoking application. The script can therefore do anything that the application's own scripts can do, such as accessing application data and performing actions within the context of the current user.

If you include a script from an external domain, then you are trusting that domain with the data and functionality of your application, and you are trusting the domain's own security to prevent an attacker from modifying the script to perform malicious actions within your application.

Issue remediation

Scripts should ideally not be included from untrusted domains. Applications that rely on static third-party scripts should consider using Subresource Integrity to make browsers verify them, or copying the contents of these scripts onto their own domain and including them from there. If that is not possible (e.g. for licensing reasons) then consider reimplementing the script's functionality within application code.

References

- Subresource Integrity

Vulnerability classifications

- CWE-829: Inclusion of Functionality from Untrusted Control Sphere

Request

```
GET / HTTP/2
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
```

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

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:07:25 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:07:25 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=e2t6%2BchWijl7%2Fy0anpYIzyfRSvcDVb1NmQNPidpPgrqAcoBxPBGdGgVZNQPiNTotKrfudY8Qu6WSOuW2RHyhatAMgB20JwxZOR7AmSIsJxl22b7gmSSnLGDwqHySvHa18Uev"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff44632b9c40a5-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet" media="screen" href="https:/
...[SNIP]...
</div><script defer src="https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015" integrity="sha512-ZpsOmlRQV6y907TI0dKBHq9Md29nnaEIPlkf84rnaERnq6zvWvPUqr2ft8M1aS28oN72PdrCzSjY4U6VaAw1EQ==" data-cf-beacon='{"rayId":"89ff44632b9c40a5","b":1,"version":"2024.4.1","token":"a72ced6cfafe44e29a8c723fdc2e2249"}' crossorigin="anonymous"></script>
...[SNIP]...
```

---

6. Frameable response (potential Clickjacking)

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://www.ourshopee.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/2
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:07:25 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:07:25 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=e2t6%2BchWijl7%2Fy0anpYIzyfRSvcDVb1NmQNPidpPgrqAcoBxPBGdGgVZNQPiNTotKrfudY8Qu6WSOuW2RHyhatAMgB20JwxZOR7AmSIsJxl22b7gmSSnLGDwqHySvHa18Uev"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff44632b9c40a5-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet" media="screen" href="https:/
...[SNIP]...
```

7. HTML5 storage manipulation (DOM-based)

There are 10 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.

HTML5 storage manipulation arises when a script stores controllable data in the HTML5 storage of the web browser (either localStorage or sessionStorage). An attacker may be able to use this behavior to construct a URL that, if visited by another application user, will cause the user's browser to store attacker-controllable data.

This behavior does not in itself constitute a security vulnerability. However, if the application later reads the data back from storage and processes it in an unsafe way, then an attacker may be able to leverage the storage mechanism to deliver other DOM-based attacks, such as cross-site scripting and JavaScript injection.

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 HTML5 storage manipulation is not to place in HTML5 storage 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.

References

- Web Security Academy: HTML5 storage manipulation (DOM-based)

Vulnerability classifications

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

7.1. https://www.ourshopee.com/

Summary

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

Issue detail

The application may be vulnerable to DOM-based HTML5 storage manipulation. Data is read from **location.href** and passed to **localStorage.setItem.value**.

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\Va.nel.cloudflare.com\/report\Vv4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2Cdd
GOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **localStorage.setItem.value**.

The following value was injected into the source:

```
https://www.ourshopee.com/?qqe0tbd2mv=qqe0tbd2mv%27%22`'"/qqe0tbd2mv/><qqe0tbd2mv/\>dget0tqq1g&#qqe0tbd2mv=qqe0tbd2mv%27%22`'"/qqe0tbd2mv/><q
```

The previous value reached the sink as:

```
{"1":{"protocol":"https:","host":"mc.yandex.ru","resource":"watch/90441013","time":1720433292123,"counterType":"0","params":{"page-url":"http
```

The stack trace at the source was:

```
at Object._0x165f99 [as proxiedGetterCallback] (<anonymous>:1:557377)
at get href (<anonymous>:1:249544)
at https://mc.yandex.ru/metrika/tag.js:165:117
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at n (https://mc.yandex.ru/metrika/tag.js:165:72)
at https://mc.yandex.ru/metrika/tag.js:150:462
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at U (https://mc.yandex.ru/metrika/tag.js:150:440)
at https://mc.yandex.ru/metrika/tag.js:226:354
at https://mc.yandex.ru/metrika/tag.js:145:407
at https://mc.yandex.ru/metrika/tag.js:145:316
at https://mc.yandex.ru/metrika/tag.js:91:221
at f (https://mc.yandex.ru/metrika/tag.js:1:123)
at https://mc.yandex.ru/metrika/tag.js:2:130
at https://mc.yandex.ru/metrika/tag.js:145:407
at new $e (https://mc.yandex.ru/metrika/tag.js:2:204)
at https://mc.yandex.ru/metrika/tag.js:401:128
at https://mc.yandex.ru/metrika/tag.js:161:496
at ua (https://mc.yandex.ru/metrika/tag.js:159:109)
at https://mc.yandex.ru/metrika/tag.js:161:427
at Array.map (<anonymous>)
at Jk (https://mc.yandex.ru/metrika/tag.js:194:325)
at https://mc.yandex.ru/metrika/tag.js:161:427
at gk (https://mc.yandex.ru/metrika/tag.js:162:25)
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at https://mc.yandex.ru/metrika/tag.js:159:220
at Array.map (<anonymous>)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.tYxZd.quoteContext [as setItem] (<anonymous>:1:453247)
at Aj (https://mc.yandex.ru/metrika/tag.js:134:131)
at Object.D (https://mc.yandex.ru/metrika/tag.js:134:4)
at Rf (https://mc.yandex.ru/metrika/tag.js:95:243)
at N (https://mc.yandex.ru/metrika/tag.js:95:96)
at Object.Md (https://mc.yandex.ru/metrika/tag.js:139:188)
at c (https://mc.yandex.ru/metrika/tag.js:142:19)
at Jj (https://mc.yandex.ru/metrika/tag.js:142:97)
```

```
at https://mc.yandex.ru/metrika/tag.js:142:44
at https://mc.yandex.ru/metrika/tag.js:13:20
```

7.2. https://www.ourshopee.com/

Summary

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

Issue detail

The application may be vulnerable to DOM-based HTML5 storage manipulation. Data is read from **document.referrer** and passed to **localStorage.setItem.value**.

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2CddGOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **document.referrer** and passed to **localStorage.setItem.value**.

The following value was injected into the source:

```
https://www.ourshopee.com/?ymr3svxj3c=ymr3svxj3c%27%22%60'%22/ymr3svxj3c/%3E%3Cymr3svxj3c/\%3Ejk0g5ir81c&
```

The previous value reached the sink as:

```
{"1":{"protocol":"https:","host":"mc.yandex.ru","resource":"watch/90441013","time":1720433292123,"counterType":"0","params":{"page-url":"http
```

The stack trace at the source was:

```
at HTMLDocument.get [as referrer] (<anonymous>:1:276163)
at https://mc.yandex.ru/metrika/tag.js:226:383
at https://mc.yandex.ru/metrika/tag.js:145:407
at https://mc.yandex.ru/metrika/tag.js:145:316
at https://mc.yandex.ru/metrika/tag.js:91:221
at f (https://mc.yandex.ru/metrika/tag.js:1:123)
at https://mc.yandex.ru/metrika/tag.js:2:130
at https://mc.yandex.ru/metrika/tag.js:145:407
at new $e (https://mc.yandex.ru/metrika/tag.js:2:204)
at https://mc.yandex.ru/metrika/tag.js:401:128
at https://mc.yandex.ru/metrika/tag.js:161:496
at ua (https://mc.yandex.ru/metrika/tag.js:159:109)
at https://mc.yandex.ru/metrika/tag.js:161:427
at Array.map (<anonymous>)
at Jk (https://mc.yandex.ru/metrika/tag.js:194:325)
at https://mc.yandex.ru/metrika/tag.js:161:427
at gk (https://mc.yandex.ru/metrika/tag.js:162:25)
at Array.reduce (<anonymous>)
```

```
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at https://mc.yandex.ru/metrika/tag.js:159:220
at Array.map (<anonymous>)
at Jk (https://mc.yandex.ru/metrika/tag.js:194:325)
at Ce (https://mc.yandex.ru/metrika/tag.js:100:40)
at https://mc.yandex.ru/metrika/tag.js:424:200
at https://mc.yandex.ru/metrika/tag.js:424:236
at https://mc.yandex.ru/metrika/tag.js:424:246
at https://mc.yandex.ru/metrika/tag.js:424:264
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.tYxZd.quoteContext [as setItem] (<anonymous>:1:453247)
at Aj (https://mc.yandex.ru/metrika/tag.js:134:131)
at Object.D (https://mc.yandex.ru/metrika/tag.js:134:4)
at Rf (https://mc.yandex.ru/metrika/tag.js:95:243)
at N (https://mc.yandex.ru/metrika/tag.js:95:96)
at Object.Md (https://mc.yandex.ru/metrika/tag.js:139:188)
at c (https://mc.yandex.ru/metrika/tag.js:142:19)
at Jj (https://mc.yandex.ru/metrika/tag.js:142:97)
at https://mc.yandex.ru/metrika/tag.js:142:44
at https://mc.yandex.ru/metrika/tag.js:13:20
```

The following proof of concept was generated for this issue:

```
<!-- Visit from your domain -->
http://your-domain?
<!-- Link back to site from your domain -->
<a href="https://www.ourshopee.com/">PoC</a>
```

7.3. https://www.ourshopee.com/

Summary

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

Issue detail

The application may be vulnerable to DOM-based HTML5 storage manipulation. Data is read from **location.href** and passed to **localStorage.setItem.value**.

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\Va.nel.cloudflare.com\Vreport\Vv4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2Cdd
GOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **localStorage.setItem.value**.

The following value was injected into the source:

```
https://www.ourshopee.com/?z6ff7jbm4r=z6ff7jbm4r%27%22`'"/z6ff7jbm4r/><z6ff7jbm4r/\>a4mi3rzf2j&#z6ff7jbm4r=z6ff7jbm4r%27%22`'"/z6ff7jbm4r/><z
```

The previous value reached the sink as:

```
{"1":{"protocol":"https:","host":"mc.yandex.ru","resource":"clmap/90441013","time":1720433316255,"counterType":"0","params":{"page-url":"http
```

The stack trace at the source was:

```
at Object._0x165f99 [as proxiedGetterCallback] (<anonymous>:1:557377)
at get href (<anonymous>:1:249544)
at https://mc.yandex.ru/metrika/tag.js:165:117
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at n (https://mc.yandex.ru/metrika/tag.js:165:72)
at https://mc.yandex.ru/metrika/tag.js:150:462
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at U (https://mc.yandex.ru/metrika/tag.js:150:440)
at https://mc.yandex.ru/metrika/tag.js:237:396
at HTMLDocument.<anonymous> (https://mc.yandex.ru/metrika/tag.js:145:407)
at _0x14405e (<anonymous>:1:147957)
at Object.MJAdz (<anonymous>:1:7812)
at _0x2a880c (<anonymous>:1:150271)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.tYxZd.quoteContext [as setItem] (<anonymous>:1:453247)
at Aj (https://mc.yandex.ru/metrika/tag.js:134:131)
at Object.D (https://mc.yandex.ru/metrika/tag.js:134:4)
at Rf (https://mc.yandex.ru/metrika/tag.js:95:243)
at N (https://mc.yandex.ru/metrika/tag.js:95:96)
at Object.Md (https://mc.yandex.ru/metrika/tag.js:139:188)
at c (https://mc.yandex.ru/metrika/tag.js:142:19)
at Jj (https://mc.yandex.ru/metrika/tag.js:142:97)
at gk (https://mc.yandex.ru/metrika/tag.js:162:25)
at https://mc.yandex.ru/metrika/tag.js:161:496
at https://mc.yandex.ru/metrika/tag.js:139:226
at new Promise (<anonymous>)
at new Ue (https://mc.yandex.ru/metrika/tag.js:204:132)
at Fj (https://mc.yandex.ru/metrika/tag.js:139:58)
at https://mc.yandex.ru/metrika/tag.js:135:377
at https://mc.yandex.ru/metrika/tag.js:135:312
at https://mc.yandex.ru/metrika/tag.js:226:29
at Xp (https://mc.yandex.ru/metrika/tag.js:92:439)
at https://mc.yandex.ru/metrika/tag.js:238:221
at HTMLDocument.<anonymous> (https://mc.yandex.ru/metrika/tag.js:145:407)
at _0x14405e (<anonymous>:1:147957)
at Object.MJAdz (<anonymous>:1:7812)
at _0x2a880c (<anonymous>:1:150271)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

This was triggered by a **click** event on an element with an id of **root** with the following HTML:

```
<div id="root"><div><div class=""><div class="header"><div class="navbar1"><div class="maxWidthConta
```

7.4. https://www.ourshopee.com/

Summary

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

Issue detail

The application may be vulnerable to DOM-based HTML5 storage manipulation. Data is read from **location.href** and passed to **localStorage.setItem.value**.

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
```

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

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2CddGOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **localStorage.setItem.value**.

The following value was injected into the source:

```
https://www.ourshopee.com/?z6ff7jbm4r=z6ff7jbm4r%27%22`'"/z6ff7jbm4r/><z6ff7jbm4r/\>a4mi3rzf2j&#z6ff7jbm4r=z6ff7jbm4r%27%22`'"/z6ff7jbm4r/><z
```

The previous value reached the sink as:

```
{"1":{"protocol":"https:","host":"mc.yandex.ru","resource":"clmap/90441013","time":1720433316255,"counterType":"0","params":{"page-url":"http
```

The stack trace at the source was:

```
at Object._0x165f99 [as proxiedGetterCallback] (<anonymous>:1:557377)
at get href (<anonymous>:1:249544)
at https://mc.yandex.ru/metrika/tag.js:165:117
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at n (https://mc.yandex.ru/metrika/tag.js:165:72)
at https://mc.yandex.ru/metrika/tag.js:150:462
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at U (https://mc.yandex.ru/metrika/tag.js:150:440)
at https://mc.yandex.ru/metrika/tag.js:237:396
at HTMLDocument.<anonymous> (https://mc.yandex.ru/metrika/tag.js:145:407)
at _0x14405e (<anonymous>:1:147957)
at Object.MJAdz (<anonymous>:1:7812)
at _0x2a880c (<anonymous>:1:150271)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.tYxZd.quoteContext [as setItem] (<anonymous>:1:453247)
at Aj (https://mc.yandex.ru/metrika/tag.js:134:131)
at Object.D (https://mc.yandex.ru/metrika/tag.js:134:4)
at Rf (https://mc.yandex.ru/metrika/tag.js:95:243)
at N (https://mc.yandex.ru/metrika/tag.js:95:96)
at Object.Md (https://mc.yandex.ru/metrika/tag.js:139:188)
at c (https://mc.yandex.ru/metrika/tag.js:142:19)
at Jj (https://mc.yandex.ru/metrika/tag.js:142:97)
at gk (https://mc.yandex.ru/metrika/tag.js:162:25)
at https://mc.yandex.ru/metrika/tag.js:161:496
at https://mc.yandex.ru/metrika/tag.js:139:226
at new Promise (<anonymous>)
at new Ue (https://mc.yandex.ru/metrika/tag.js:204:132)
at Fj (https://mc.yandex.ru/metrika/tag.js:139:58)
at https://mc.yandex.ru/metrika/tag.js:135:377
at https://mc.yandex.ru/metrika/tag.js:135:312
at https://mc.yandex.ru/metrika/tag.js:226:29
at Xp (https://mc.yandex.ru/metrika/tag.js:92:439)
at https://mc.yandex.ru/metrika/tag.js:238:221
at HTMLDocument.<anonymous> (https://mc.yandex.ru/metrika/tag.js:145:407)
at _0x14405e (<anonymous>:1:147957)
at _0x2a880c (<anonymous>:1:151903)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

This was triggered by a **click** event with the following HTML:

```
<svg stroke="currentColor" fill="currentColor" stroke-width="0" viewBox="0 0 20 20" class="menuBar d
```

7.5. https://www.ourshopee.com/

Summary

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

Issue detail

The application may be vulnerable to DOM-based HTML5 storage manipulation. Data is read from **location.href** and passed to **localStorage.setItem.value**.

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2Cdd
GOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **localStorage.setItem.value**.

The following value was injected into the source:

```
https://www.ourshopee.com/?htg49oxuc8=htg49oxuc8%27%22`'"/htg49oxuc8/><htg49oxuc8/\>vqjw4xytvs&#htg49oxuc8=htg49oxuc8%27%22`'"/htg49oxuc8/><h
```

The previous value reached the sink as:

```
{"1":{"protocol":"https:","host":"mc.yandex.ru","resource":"clmap/90441013","time":1720433316255,"counterType":"0","params":{"page-url":"http
```

The stack trace at the source was:

```
at Object._0x165f99 [as proxiedGetterCallback] (<anonymous>:1:557377)
at get href (<anonymous>:1:249544)
at https://mc.yandex.ru/metrika/tag.js:165:117
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at n (https://mc.yandex.ru/metrika/tag.js:165:72)
at https://mc.yandex.ru/metrika/tag.js:150:462
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at U (https://mc.yandex.ru/metrika/tag.js:150:440)
at https://mc.yandex.ru/metrika/tag.js:237:396
at HTMLDocument.<anonymous> (https://mc.yandex.ru/metrika/tag.js:145:407)
at _0x14405e (<anonymous>:1:147957)
at _0x2a880c (<anonymous>:1:151903)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
```

```
at _0xdc6a5f.tYxZd.quoteContext [as setItem] (<anonymous>:1:453247)
at Aj (https://mc.yandex.ru/metrika/tag.js:134:131)
at Object.D (https://mc.yandex.ru/metrika/tag.js:134:4)
at Rf (https://mc.yandex.ru/metrika/tag.js:95:243)
at N (https://mc.yandex.ru/metrika/tag.js:95:96)
at Object.Md (https://mc.yandex.ru/metrika/tag.js:139:188)
at c (https://mc.yandex.ru/metrika/tag.js:142:19)
at Jj (https://mc.yandex.ru/metrika/tag.js:142:97)
at gk (https://mc.yandex.ru/metrika/tag.js:162:25)
at https://mc.yandex.ru/metrika/tag.js:161:496
at https://mc.yandex.ru/metrika/tag.js:139:226
at new Promise (<anonymous>)
at new Ue (https://mc.yandex.ru/metrika/tag.js:204:132)
at Fj (https://mc.yandex.ru/metrika/tag.js:139:58)
at https://mc.yandex.ru/metrika/tag.js:135:377
at https://mc.yandex.ru/metrika/tag.js:135:312
at https://mc.yandex.ru/metrika/tag.js:226:29
at Xp (https://mc.yandex.ru/metrika/tag.js:92:439)
at https://mc.yandex.ru/metrika/tag.js:238:221
at HTMLDocument.<anonymous> (https://mc.yandex.ru/metrika/tag.js:145:407)
at _0x14405e (<anonymous>:1:147957)
at _0x2a880c (<anonymous>:1:151903)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

This was triggered by a **click** event with the following HTML:

```
<svg stroke="currentColor" fill="currentColor" stroke-width="0" viewBox="0 0 20 20" class="menuBar d
```

7.6. https://www.ourshopee.com/

Summary

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

Issue detail

The application may be vulnerable to DOM-based HTML5 storage manipulation. Data is read from **location.href** and passed to **localStorage.setItem.value**.

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2Cdd
GOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **localStorage.setItem.value**.

The following value was injected into the source:

```
https://www.ourshopee.com/?bzn755fnbj=bzn755fnbj%27%22`'"/bzn755fnbj/><bzn755fnbj/\>ggjv1ijrqj&#bzn755fnbj=bzn755fnbj%27%22`'"/bzn755fnbj/><b
```

The previous value reached the sink as:

{"1":{"protocol":"https:","host":"mc.yandex.ru","resource":"clmap/90441013","time":1720433316255,"counterType":"0","params":{"page-url":"http

The stack trace at the source was:

```
at Object._0x165f99 [as proxiedGetterCallback] (<anonymous>:1:557377)
at get href (<anonymous>:1:249544)
at https://mc.yandex.ru/metrika/tag.js:165:117
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at n (https://mc.yandex.ru/metrika/tag.js:165:72)
at https://mc.yandex.ru/metrika/tag.js:150:462
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at U (https://mc.yandex.ru/metrika/tag.js:150:440)
at https://mc.yandex.ru/metrika/tag.js:235:330
at e (https://mc.yandex.ru/metrika/tag.js:170:358)
at f (https://mc.yandex.ru/metrika/tag.js:170:458)
at HTMLDocument.d (https://mc.yandex.ru/metrika/tag.js:170:329)
at _0x14405e (<anonymous>:1:147957)
at Object.MJAdz (<anonymous>:1:7812)
at _0x2a880c (<anonymous>:1:150271)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.tYxZd.quoteContext [as setItem] (<anonymous>:1:453247)
at Aj (https://mc.yandex.ru/metrika/tag.js:134:131)
at Object.D (https://mc.yandex.ru/metrika/tag.js:134:4)
at Rf (https://mc.yandex.ru/metrika/tag.js:95:243)
at N (https://mc.yandex.ru/metrika/tag.js:95:96)
at Object.Md (https://mc.yandex.ru/metrika/tag.js:139:188)
at c (https://mc.yandex.ru/metrika/tag.js:142:19)
at Jj (https://mc.yandex.ru/metrika/tag.js:142:97)
at https://mc.yandex.ru/metrika/tag.js:142:44
at https://mc.yandex.ru/metrika/tag.js:83:415
```

7.7. https://www.ourshopee.com/

Summary

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

Issue detail

The application may be vulnerable to DOM-based HTML5 storage manipulation. Data is read from **location.href** and passed to **localStorage.setItem.value**.

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2CddGOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400
```

```
<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **localStorage.setItem.value**.

The following value was injected into the source:

```
https://www.ourshopee.com/?z6ff7jbm4r=z6ff7jbm4r%27%22`'"/z6ff7jbm4r/><z6ff7jbm4r/\>a4mi3rzf2j&#z6ff7jbm4r=z6ff7jbm4r%27%22`'"/z6ff7jbm4r/><z
```

The previous value reached the sink as:

```
{"1":{"protocol":"https:","host":"mc.yandex.ru","resource":"clmap/90441013","time":1720433316255,"counterType":"0","params":{"page-url":"http
```

The stack trace at the source was:

```
at Object._0x165f99 [as proxiedGetterCallback] (<anonymous>:1:557377)
at get href (<anonymous>:1:249544)
at https://mc.yandex.ru/metrika/tag.js:165:117
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at n (https://mc.yandex.ru/metrika/tag.js:165:72)
at https://mc.yandex.ru/metrika/tag.js:150:462
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at U (https://mc.yandex.ru/metrika/tag.js:150:440)
at https://mc.yandex.ru/metrika/tag.js:237:396
at HTMLDocument.<anonymous> (https://mc.yandex.ru/metrika/tag.js:145:407)
at _0x14405e (<anonymous>:1:147957)
at Object.MJAdz (<anonymous>:1:7812)
at _0x2a880c (<anonymous>:1:150271)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.tYxZd.quoteContext [as setItem] (<anonymous>:1:453247)
at Aj (https://mc.yandex.ru/metrika/tag.js:134:131)
at Object.D (https://mc.yandex.ru/metrika/tag.js:134:4)
at Rf (https://mc.yandex.ru/metrika/tag.js:95:243)
at N (https://mc.yandex.ru/metrika/tag.js:95:96)
at Object.Md (https://mc.yandex.ru/metrika/tag.js:139:188)
at c (https://mc.yandex.ru/metrika/tag.js:142:19)
at Jj (https://mc.yandex.ru/metrika/tag.js:142:97)
at https://mc.yandex.ru/metrika/tag.js:142:44
at https://mc.yandex.ru/metrika/tag.js:83:415
```

This was triggered by a **click** event with the following HTML:

```
<svg stroke="currentColor" fill="currentColor" stroke-width="0" viewBox="0 0 20 20" class="menuBar d
```

7.8. https://www.ourshopee.com/

Summary

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

Issue detail

The application may be vulnerable to DOM-based HTML5 storage manipulation. Data is read from **location.href** and passed to **localStorage.setItem.value**.

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2CddGOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet" media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **localStorage.setItem.value**.

The following value was injected into the source:

```
https://www.ourshopee.com/?htg49oxuc8=htg49oxuc8%27%22`'"/htg49oxuc8/><htg49oxuc8/\>vqjw4xytvs&#htg49oxuc8=htg49oxuc8%27%22`'"/htg49oxuc8/><h
```

The previous value reached the sink as:

```
{"1":{"protocol":"https:","host":"mc.yandex.ru","resource":"clmap/90441013","time":1720433316255,"counterType":"0","params":{"page-url":"http
```

The stack trace at the source was:

```
at Object._0x165f99 [as proxiedGetterCallback] (<anonymous>:1:557377)
at get href (<anonymous>:1:249544)
at https://mc.yandex.ru/metrika/tag.js:165:117
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at n (https://mc.yandex.ru/metrika/tag.js:165:72)
at https://mc.yandex.ru/metrika/tag.js:150:462
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at U (https://mc.yandex.ru/metrika/tag.js:150:440)
at https://mc.yandex.ru/metrika/tag.js:237:396
at HTMLDocument.<anonymous> (https://mc.yandex.ru/metrika/tag.js:145:407)
at _0x14405e (<anonymous>:1:147957)
at _0x2a880c (<anonymous>:1:151903)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.tYxZd.quoteContext [as setItem] (<anonymous>:1:453247)
at Aj (https://mc.yandex.ru/metrika/tag.js:134:131)
at Object.D (https://mc.yandex.ru/metrika/tag.js:134:4)
at Rf (https://mc.yandex.ru/metrika/tag.js:95:243)
at N (https://mc.yandex.ru/metrika/tag.js:95:96)
at Object.Md (https://mc.yandex.ru/metrika/tag.js:139:188)
at c (https://mc.yandex.ru/metrika/tag.js:142:19)
at Jj (https://mc.yandex.ru/metrika/tag.js:142:97)
at https://mc.yandex.ru/metrika/tag.js:142:44
at https://mc.yandex.ru/metrika/tag.js:83:415
```

This was triggered by a **click** event with the following HTML:

```
<svg stroke="currentColor" fill="currentColor" stroke-width="0" viewBox="0 0 20 20" class="menuBar d
```

7.9. https://www.ourshopee.com/

Summary

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

Issue detail

The application may be vulnerable to DOM-based HTML5 storage manipulation. Data is read from **location.href** and passed to **localStorage.setItem.value**.

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2Cdd
GOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **localStorage.setItem.value**.

The following value was injected into the source:

```
https://www.ourshopee.com/?z6ff7jbm4r=z6ff7jbm4r%27%22`'"/z6ff7jbm4r/><z6ff7jbm4r/\>a4mi3rzf2j&#z6ff7jbm4r=z6ff7jbm4r%27%22`'"/z6ff7jbm4r/><z
```

The previous value reached the sink as:

```
{"1":{"protocol":"https:","host":"mc.yandex.ru","resource":"clmap/90441013","time":1720433316255,"counterType":"0","params":{"page-url":"http
```

The stack trace at the source was:

```
at Object._0x165f99 [as proxiedGetterCallback] (<anonymous>:1:557377)
at get href (<anonymous>:1:249544)
at https://mc.yandex.ru/metrika/tag.js:165:117
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at n (https://mc.yandex.ru/metrika/tag.js:165:72)
at https://mc.yandex.ru/metrika/tag.js:150:462
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at U (https://mc.yandex.ru/metrika/tag.js:150:440)
at https://mc.yandex.ru/metrika/tag.js:237:396
at HTMLDocument.<anonymous> (https://mc.yandex.ru/metrika/tag.js:145:407)
at _0x14405e (<anonymous>:1:147957)
at Object.MJAdz (<anonymous>:1:7812)
at _0x2a880c (<anonymous>:1:150271)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at _0xdc6a5f.tYxZd.quoteContext [as setItem] (<anonymous>:1:453247)
at Aj (https://mc.yandex.ru/metrika/tag.js:134:131)
at Object.D (https://mc.yandex.ru/metrika/tag.js:134:4)
at Rf (https://mc.yandex.ru/metrika/tag.js:95:243)
at Vi (https://mc.yandex.ru/metrika/tag.js:95:203)
at Ba (https://mc.yandex.ru/metrika/tag.js:95:124)
at Object.Md (https://mc.yandex.ru/metrika/tag.js:139:188)
at c (https://mc.yandex.ru/metrika/tag.js:142:19)
at Jj (https://mc.yandex.ru/metrika/tag.js:142:97)
at gk (https://mc.yandex.ru/metrika/tag.js:162:25)
at https://mc.yandex.ru/metrika/tag.js:161:496
at https://mc.yandex.ru/metrika/tag.js:139:226
at new Promise (<anonymous>)
at new Ue (https://mc.yandex.ru/metrika/tag.js:204:132)
at Fj (https://mc.yandex.ru/metrika/tag.js:139:58)
at https://mc.yandex.ru/metrika/tag.js:136:117
```

This was triggered by a **click** event with the following HTML:

```
<svg stroke="currentColor" fill="currentColor" stroke-width="0" viewBox="0 0 20 20" class="menuBar d
```

7.10. https://www.ourshopee.com/

Summary

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

Issue detail

The application may be vulnerable to DOM-based HTML5 storage manipulation. Data is read from **location.href** and passed to **localStorage.setItem.value**.

Request

```
GET / HTTP/1.1
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:01 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:05:01 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vfH4YkCg6jQfNHKTm1hYUraAj2JZUGAN2tl%2BRE17sCm4sUO9Mnd%2FkaE13grELUN4KEFUSMQl3Avs1%2BfVCY9cJuNJdHCSQaDi44l4qe4AEkro%2BWvv9r75d%2B3nM9p2Cdd
GOi%2Fo"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff40e36d313e40-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **localStorage.setItem.value**.

The following value was injected into the source:

```
https://www.ourshopee.com/?htg49oxuc8=htg49oxuc8%27%22`'"/htg49oxuc8/><htg49oxuc8/\>vqjw4xytvs&#htg49oxuc8=htg49oxuc8%27%22`'"/htg49oxuc8/><h
```

The previous value reached the sink as:

```
{"1":{"protocol":"https:","host":"mc.yandex.ru","resource":"clmap/90441013","time":1720433316255,"counterType":"0","params":{"page-url":"http
```

The stack trace at the source was:

```
at Object._0x165f99 [as proxiedGetterCallback] (<anonymous>:1:557377)
at get href (<anonymous>:1:249544)
at https://mc.yandex.ru/metrika/tag.js:165:117
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at n (https://mc.yandex.ru/metrika/tag.js:165:72)
at https://mc.yandex.ru/metrika/tag.js:150:462
at Array.reduce (<anonymous>)
at yb (https://mc.yandex.ru/metrika/tag.js:192:163)
at U (https://mc.yandex.ru/metrika/tag.js:150:440)
at https://mc.yandex.ru/metrika/tag.js:237:396
at HTMLDocument.<anonymous> (https://mc.yandex.ru/metrika/tag.js:145:407)
at _0x14405e (<anonymous>:1:147957)
at _0x2a880c (<anonymous>:1:151903)
at Object.fEpIW (<anonymous>:1:94004)
at _0x4ca456 (<anonymous>:1:574787)
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
```

```
at _0xdc6a5f.tYxZd.quoteContext [as setItem] (<anonymous>:1:453247)
at Aj (https://mc.yandex.ru/metrika/tag.js:134:131)
at Object.D (https://mc.yandex.ru/metrika/tag.js:134:4)
at Rf (https://mc.yandex.ru/metrika/tag.js:95:243)
at Vi (https://mc.yandex.ru/metrika/tag.js:95:203)
at Ba (https://mc.yandex.ru/metrika/tag.js:95:124)
at Object.Md (https://mc.yandex.ru/metrika/tag.js:139:188)
at c (https://mc.yandex.ru/metrika/tag.js:142:19)
at Jj (https://mc.yandex.ru/metrika/tag.js:142:97)
at gk (https://mc.yandex.ru/metrika/tag.js:162:25)
at https://mc.yandex.ru/metrika/tag.js:161:496
at https://mc.yandex.ru/metrika/tag.js:139:226
at new Promise (<anonymous>)
at new Ue (https://mc.yandex.ru/metrika/tag.js:204:132)
at Fj (https://mc.yandex.ru/metrika/tag.js:139:58)
at https://mc.yandex.ru/metrika/tag.js:136:117
```

This was triggered by a **click** event with the following HTML:

```
<svg stroke="currentColor" fill="currentColor" stroke-width="0" viewBox="0 0 20 20" class="menuBar d
```

---

8. Email addresses disclosed

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://www.ourshopee.com**
Path:	**/locales/en/translation.json**

Issue detail

The following email address was disclosed in the response:

- support@ourshopee.com

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

References

- Web Security Academy: Information disclosure

Vulnerability classifications

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

Request

```
GET /locales/en/translation.json HTTP/2
Host: www.ourshopee.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/126.0.6478.127 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://www.ourshopee.com/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:07:25 GMT
Content-Type: application/json
Last-Modified: Tue, 07 May 2024 09:55:57 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:07:25 GMT
```

```
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=osoTdhZKF%2BgTE0RfERvYR73Hi8etd1q%2BaKBq0Q%2B%2FcclPRHWx%2BZ97WfFTwLY%2FcLoNOf143pBnUQQu%2BP2Vddw6vLPLtLMEOAfXCSeKpdOfuLMKFAiE%2Bmdqkg
GE4%2By81%2BUqbSDW"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff4467af8e40a5-BOM
Alt-Svc: h3=":443"; ma=86400

{
"localization_testing": "ENGLISH",
"global.viewAll": "View All",
"global.addCart": "ADD TO CART",
"global.off": "OFF",

"home.excitingTitle": "Exciting Offers",
"home.
...[SNIP]...
cess to all information related to such account, including but not limited to, orders, returns, warranty.",
"delete.term3" : "For any other queries or clarifications, please reach out to customer support@ourshopee.com",
"delete.youraccount" : "Delete Your Account"


}
```

---

9. Robots.txt file

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://www.ourshopee.com**
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: www.ourshopee.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/126.0.6478.127 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 08 Jul 2024 10:08:10 GMT
Content-Type: text/plain
Connection: close
Last-Modified: Thu, 02 May 2024 10:39:54 GMT
Cache-Control: max-age=31536000
Expires: Thu, 25 Jul 2024 17:54:35 GMT
CF-Cache-Status: HIT
Age: 805045
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=dtgz6JP%2FOBvfAkRHibawrE9wFkYmkjDwKs6eyfTLNrNOrkVcpxcQDVHyo6uA165M8ancD8YIYCaVUtmVQ1uyrMx407%2FX8uVgPeI8Yx9wfiPUpmW7P%2FoGsk%2FQY7HvCIVr%2B
r7Q"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 89ff45803fe74226-BOM
```

```
alt-svc: h3=":443"; ma=86400
Content-Length: 70

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

---

10. Cacheable HTTPS response

There are 3 instances of this issue:

- /
- /locales/en/translation.json
- /robots.txt

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

10.1. https://www.ourshopee.com/

Summary

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

Request

```
GET / HTTP/2
Host: www.ourshopee.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/126.0.6478.127 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="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:07:25 GMT
Content-Type: text/html
Last-Modified: Tue, 07 May 2024 13:53:36 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:07:25 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=e2t6%2BchWijl7%2Fy0anpYIzyfRSvcDVb1NmQNPidpPgrqAcoBxPBGdGgVZNQPiNTotKrfudY8Qu6WSOuW2RHyhatAMgB20JwxZOR7AmSIsJxl22b7gmSSnLGDwqHySvHa18Uev"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
```

```
Server: cloudflare
Cf-Ray: 89ff44632b9c40a5-BOM
Alt-Svc: h3=":443"; ma=86400

<!doctype html><html lang="en"><head><meta charset="utf-8" /><link rel="icon" type="image/png" href="https://www.ourshopee.com/Assets/favicon.png" /><link rel="stylesheet"
media="screen" href="https:/
...[SNIP]...
```

10.2. https://www.ourshopee.com/locales/en/translation.json

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://www.ourshopee.com**
Path:	**/locales/en/translation.json**

Request

```
GET /locales/en/translation.json HTTP/2
Host: www.ourshopee.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/126.0.6478.127 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://www.ourshopee.com/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="126", "Chromium";v="126"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:07:25 GMT
Content-Type: application/json
Last-Modified: Tue, 07 May 2024 09:55:57 GMT
Cache-Control: max-age=2678400
Expires: Thu, 08 Aug 2024 10:07:25 GMT
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=osoTdhZKF%2BgTE0RfERvYR73Hi8etd1q%2BaKBq0Q%2B%2FcclPRHWx%2BZ97WfFTwLY%2FcLoNOf143pBnUQQu%2BP2Vddw6vLPLtLMEOAfXCSeKpdOfuLMKFAiE%2Bmdqkg
GE4%2By81%2BUqbSDW"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 89ff4467af8e40a5-BOM
Alt-Svc: h3=":443"; ma=86400

{
"localization_testing": "ENGLISH",
"global.viewAll": "View All",
"global.addCart": "ADD TO CART",
"global.off": "OFF",

"home.excitingTitle": "Exciting Offers",
"home.
...[SNIP]...
```

10.3. https://www.ourshopee.com/robots.txt

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://www.ourshopee.com**
Path:	**/robots.txt**

Request

```
GET /robots.txt HTTP/2
Host: www.ourshopee.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/126.0.6478.127 Safari/537.36
Connection: close
```

```
Cache-Control: max-age=0
```

Response

```
HTTP/2 200 OK
Date: Mon, 08 Jul 2024 10:05:18 GMT
Content-Type: text/plain
Last-Modified: Thu, 02 May 2024 10:39:54 GMT
Cache-Control: max-age=31536000
Expires: Thu, 25 Jul 2024 17:54:35 GMT
Cf-Cache-Status: HIT
Age: 804873
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=xkK3EqKYRJHQ8Uj8Re78w1Y%2BxuE1g38QfL04DqJCqsv0%2BCeSkVY4sn5tOmvBxTQ4ljnSK2AqZgcmVQuuqLNN0mLPv0KZRdZpbBfsunPeCG9O8mFQ7tLYpx1Fpg%2Bad7rMQyg
7"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Vary: Accept-Encoding
Server: cloudflare
Cf-Ray: 89ff414c1ee13e40-BOM
Alt-Svc: h3=":443"; ma=86400

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

---

11. TLS certificate

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://www.ourshopee.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:	ourshopee.com, saudi.ourshopee.com, www.saudi.ourshopee.com, www.bahrain.ourshopee.com, www.kuwait.ourshopee.com, www.oman.ourshopee.com, www.qatar.ourshopee.com, *.ourshopee.com
Issued by:	WE1
Valid from:	Fri Jun 28 06:46:26 IST 2024
Valid to:	Thu Sep 26 07:45:58 IST 2024

Certificate chain #1

Issued to:	WE1
Issued by:	GTS Root R4
Valid from:	Wed Dec 13 14:30:00 IST 2023
Valid to:	Tue Feb 20 19:30:00 IST 2029

Certificate chain #2

Issued to:	GTS Root R4
Issued by:	GlobalSign Root CA
Valid from:	Wed Nov 15 09:13:21 IST 2023
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

Report generated by Burp Suite web vulnerability scanner v2024.5.5, at Mon Jul 08 15:42:34 IST 2024.