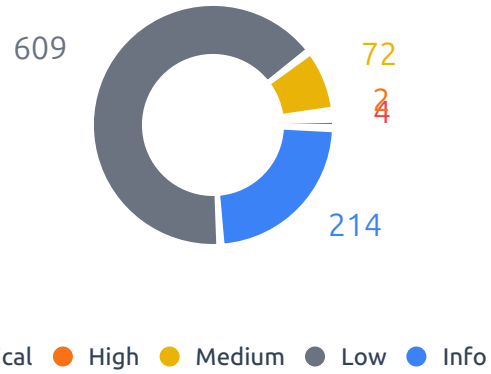
Security Audit Report

Target: ginandjuice.shop

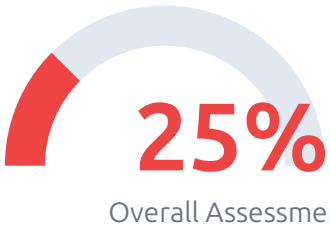
Scan Date: 11/25/2025

This document presents the findings of a comprehensive security assessment conducted on the target infrastructure. The analysis includes a **Vulnerability Assessment (VA)** phase, identifying known CVEs, open ports, and misconfigurations, followed by an automated **Penetration Testing (PT)** phase performing active attacks (e.g., XSS, SQLi) to validate security posture. The goal is to highlight critical risks and provide actionable remediation strategies.

Severity Distribution



Security Score



Open Ports

Totali: 3

Critiche: 0

CVE Summary

Totali: 1
Critiche: 1

HTTP Headers

Missing: 10
Misconfigured: 0
OK: 2

Vulnerability Assessment

Server & Info

Server Info

Domain	ginandjuice.shop
IP Address	34.249.203.140
Timestamp of scan	25/11/2025, 17:10:27
Server Version	Non specificato
Status Code server	200 OK

ALLOWED METHODS

GET

Security Headers

Header Name	Value / Details	Status
Content-Security-Policy	Not Present	✗
Strict-Transport-Security	Not Present	✗
X-Content-Type-Options	Not Present	✗
X-Frame-Options	Correctly Configured	✓
Permissions-Policy	Not Present	✗
Referrer-Policy	Not Present	✗
Cache-Control	Not Present	✗
Set-Cookie	Correctly Configured	✓
Access-Control-Allow-Origin	Not Present	✗
Cross-Origin-Opener-Policy	Not Present	✗
Cross-Origin-Embedder-Policy	Not Present	✗
Cross-Origin-Resource-Policy	Not Present	✗

Secure Weak Missing

Open Ports

Port / Proto	Service	Software Detected	State
53 TCP	Domain	dnsmasq 2.84rc2	OPEN
80 TCP	Http	awselb/2.0	OPEN
443 TCP	Https	— Unknown —	OPEN

CVE Overview

Vulnerabilità Rilevate 1

Lista delle CVE note identificate analizzando le versioni software.

CVE ID	Severity	Product	Actions
CVE-2024-10125 EXPLOIT	9.8	aws-alb-identity-middleware aws-alb-identity-middleware (All Versions)	View Details

Penetration Testing (ZAP)

OWASP ZAP Report

Results of the automatic penetration test

Cross Site Scripting (DOM Based)

Hit **3** resources

DESCRIPTION

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology.
When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise.
There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash. Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code.

RECOMMENDED SOLUTION

Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.
Phases: Implementation; Architecture and Design
Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.
For any data that will be output to another web page, especially any data that was received

from external inputs, use the appropriate encoding on all non-alphanumeric characters. Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed.
Phase: Architecture and Design
For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.
If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.
Phase: Implementation
For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping.
To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.
Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.
When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."
Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.

AFFECTED RESOURCES (3)

Method	URL	Param	Attack Payload (Snippet)
GET	https://ginandjuice.shop/login#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3	-	#jaVasCript:/*-/*`/*\`/*'/*…

	e		
GET	https://ginandjuice.shop/my-account#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e	-	#jaVasCript:/*-/*`/*\`/*'/*…
POST	https://ginandjuice.shop/login#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e	-	#jaVasCript:/*-/*`/*\`/*'/*…

Cross Site Scripting (Reflected)

Hit **1** resource

DESCRIPTION

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology.
When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise.
There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash. Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any

additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code.

RECOMMENDED SOLUTION

Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.
Phases: Implementation; Architecture and Design
Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.
For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters. Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed.
Phase: Architecture and Design
For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.
If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.
Phase: Implementation
For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping.
To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.
Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list).

Vulnerable JS Library

Absence of Anti-CSRF Tokens

Hit **36** resources

DESCRIPTION

No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.
CSRF attacks are effective in a number of situations, including:
* The victim has an active session on the target site.
* The victim is authenticated via HTTP auth on the target site.
* The victim is on the same local network as the target site.
CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

RECOMMENDED SOLUTION

Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard.
Phase: Implementation
Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.
Phase: Architecture and Design
Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).
Note that this can be bypassed using XSS.
Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.
Note that this can be bypassed using XSS.
Use the ESAPI Session Management control.
This control includes a component for CSRF.
Do not use the GET method for any request that triggers a state change.
Phase: Implementation
Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

AFFECTED RESOURCES (36)

Method	URL	Param	Attack Payload (Snippet)
GET	https://ginandjuice.shop/catalog/product?productId=1	-	
GET	https://ginandjuice.shop/catalog/product?productId=1	-	
GET	https://ginandjuice.shop/catalog/product?productId=10	-	
GET	https://ginandjuice.shop/catalog/product?productId=10	-	
GET	https://ginandjuice.shop/catalog/product?productId=11	-	
GET	https://ginandjuice.shop/catalog/product?productId=11	-	
GET	https://ginandjuice.shop/catalog/product?productId=12	-	
GET	https://ginandjuice.shop/catalog/product?productId=12	-	
GET	https://ginandjuice.shop/catalog/product?productId=13	-	
GET	https://ginandjuice.shop/catalog/product?productId=13	-	
GET	https://ginandjuice.shop/catalog/product?productId=14	-	
GET	https://ginandjuice.shop/catalog/product?productId=14	-	
GET	https://ginandjuice.shop/catalog/product?productId=15	-	
GET	https://ginandjuice.shop/catalog/product?productId=15	-	
GET	https://ginandjuice.shop/catalog/product?productId=16	-	
GET	https://ginandjuice.shop/catalog/product?productId=16	-	
GET	https://ginandjuice.shop/catalog/product?productId=17	-	
GET	https://ginandjuice.shop/catalog/product?productId=17	-	
GET	https://ginandjuice.shop/catalog/product?productId=18	-	

GET	https://ginandjuice.shop/catalog/product?productId=18	-
GET	https://ginandjuice.shop/catalog/product?productId=2	-
GET	https://ginandjuice.shop/catalog/product?productId=2	-
GET	https://ginandjuice.shop/catalog/product?productId=3	-
GET	https://ginandjuice.shop/catalog/product?productId=3	-
GET	https://ginandjuice.shop/catalog/product?productId=4	-
GET	https://ginandjuice.shop/catalog/product?productId=4	-
GET	https://ginandjuice.shop/catalog/product?productId=5	-
GET	https://ginandjuice.shop/catalog/product?productId=5	-
GET	https://ginandjuice.shop/catalog/product?productId=6	-
GET	https://ginandjuice.shop/catalog/product?productId=6	-
GET	https://ginandjuice.shop/catalog/product?productId=7	-
GET	https://ginandjuice.shop/catalog/product?productId=7	-
GET	https://ginandjuice.shop/catalog/product?productId=8	-
GET	https://ginandjuice.shop/catalog/product?productId=8	-
GET	https://ginandjuice.shop/catalog/product?productId=9	-
GET	https://ginandjuice.shop/catalog/product?productId=9	-

Content Security Policy (CSP) Header Not Set

Hit **36** resources

DESCRIPTION

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

RECOMMENDED SOLUTION

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

AFFECTED RESOURCES (36)

Method	URL	Param	Attack Payload (Snippet)
GET	https://ginandjuice.shop	-	
GET	https://ginandjuice.shop/	-	
GET	https://ginandjuice.shop/about	-	
GET	https://ginandjuice.shop/blog	-	
GET	https://ginandjuice.shop/blog/?back=https%3A%2F%2Fzap.example.com&search=ZAP	-	
GET	https://ginandjuice.shop/blog/post?postId=1	-	
GET	https://ginandjuice.shop/blog/post?postId=2	-	
GET	https://ginandjuice.shop/blog/post?postId=3	-	
GET	https://ginandjuice.shop/blog/post?postId=4	-	
GET	https://ginandjuice.shop/blog/post?postId=5	-	
GET	https://ginandjuice.shop/blog/post?postId=6	-	
GET	https://ginandjuice.shop/catalog	-	
GET	https://ginandjuice.shop/catalog/cart	-	
GET	https://ginandjuice.shop/catalog/product?productId=1	-	
GET	https://ginandjuice.shop/catalog/product?productId=10	-	

GET	https://ginandjuice.shop/catalog/product?productId=11	-
GET	https://ginandjuice.shop/catalog/product?productId=12	-
GET	https://ginandjuice.shop/catalog/product?productId=13	-
	https://ginandjuice.shop/catalo	

Cookie No HttpOnly Flag

Hit **176** resources

DESCRIPTION

A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

RECOMMENDED SOLUTION

Ensure that the HttpOnly flag is set for all cookies.

AFFECTED RESOURCES (176)

Method	URL	Param	Attack Payload (Snippet)
GET	https://ginandjuice.shop	AWSALB	
GET	https://ginandjuice.shop	AWSALBCORS	
GET	https://ginandjuice.shop/	AWSALB	
GET	https://ginandjuice.shop/	AWSALBCORS	
GET	https://ginandjuice.shop/about	AWSALB	
GET	https://ginandjuice.shop/about	AWSALBCORS	
GET	https://ginandjuice.shop/blog	AWSALB	
GET	https://ginandjuice.shop/blog	AWSALBCORS	
GET	https://ginandjuice.shop/blog/?back=https%3A%2F%2Fzap.example.com&search=ZAP	AWSALB	
GET	https://ginandjuice.shop/blog/?back=https%3A%2F%2Fzap.example.com&search=ZAP	AWSALBCORS	
GET	https://ginandjuice.shop/blog/pos	AWSALB	

GET	t?postId=1	AWSALB
GET	https://ginandjuice.shop/blog/post?postId=1	AWSALBCORS
GET	https://ginandjuice.shop/blog/post?postId=2	AWSALB
GET	https://ginandjuice.shop/blog/post?postId=2	AWSALBCORS
GET	https://ginandjuice.shop/blog/post?postId=3	AWSALB
GET	https://ginandjuice.shop/blog/post?postId=3	AWSALBCORS
GET	https://ginandjuice.shop/blog/post?postId=4	AWSALB
GET	https://ginandjuice.shop/blog/post?postId=4	AWSALBCORS
GET	https://ginandjuice.shop/blog/post?postId=5	AWSALB
GET	https://ginandjuice.shop/blog/post?postId=5	AWSALBCORS
GET	https://ginandjuice.shop/blog/post?postId=6	AWSALB
GET	https://ginandjuice.shop/blog/post?postId=6	AWSALBCORS
GET	https://ginandjuice.shop/catalog	AWSALB
GET	https://ginandjuice.shop/catalog	AWSALBCORS
GET	https://ginandjuice.shop/catalog/cart	AWSALB
GET	https://ginandjuice.shop/catalog/cart	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=1	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=1	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=10	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=10	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=11	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=11	AWSALBCORS

GET	https://ginandjuice.shop/catalog/product?productId=12	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=12	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=13	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=13	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=14	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=14	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=15	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=15	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=16	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=16	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=17	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=17	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=18	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=18	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=2	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=2	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=3	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=3	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=4	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=4	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=5	AWSALB

	product?productId=5	
GET	https://ginandjuice.shop/catalog/product?productId=5	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=6	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=6	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=7	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=7	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=8	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=8	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=9	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=9	AWSALBCORS
GET	https://ginandjuice.shop/catalog?searchTerm=ZAP	AWSALB
GET	https://ginandjuice.shop/catalog?searchTerm=ZAP	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/1.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/1.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/2.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/2.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/3.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/3.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/4.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/4.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/5.jpg	AWSALB
	https://ginandjuice.shop/image/sc	

GET	anme/blog/posts/5.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/6.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/6.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/1.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/1.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/10.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/10.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/11.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/11.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/12.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/12.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/2.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/2.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/3.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/3.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/4.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/4.pn	AWSALBCORS

	g	
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/5.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/5.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/6.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/6.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/7.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/7.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/8.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/8.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/9.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/9.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/batch_1337.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/batch_1337.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/kettle_still.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/kettle_still.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/lost_in_a_heyes.png	AWSALB
	https://ginandjuice.shop/image/sc	

GET	https://ginandjuice.shop/image/scanme/productcatalog/products/lost_in_a_heyes.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/original_dry_sqli.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/original_dry_sqli.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/pineapple_edition.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/pineapple_edition.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/purple_hat.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/purple_hat.png	AWSALBCORS
GET	https://ginandjuice.shop/login	AWSALB
GET	https://ginandjuice.shop/login	AWSALBCORS
GET	https://ginandjuice.shop/my-account	AWSALB
GET	https://ginandjuice.shop/my-account	AWSALBCORS
GET	https://ginandjuice.shop/resources/css/labsBlog.css	AWSALB
GET	https://ginandjuice.shop/resources/css/labsBlog.css	AWSALBCORS
GET	https://ginandjuice.shop/resources/css/labsEcommerce.css	AWSALB
GET	https://ginandjuice.shop/resources/css/labsEcommerce.css	AWSALBCORS
GET	https://ginandjuice.shop/resources/css/labsScanme.css	AWSALB
GET	https://ginandjuice.shop/resources/css/labsScanme.css	AWSALBCORS
GET	https://ginandjuice.shop/resources/footer/js/scanme.js	AWSALB
GET	https://ginandjuice.shop/resources/footer/js/scanme.js	AWSALBCORS
GET	https://ginandjuice.shop/resource	

GET	s/images/avatar.svg	AWSALB
GET	https://ginandjuice.shop/resources/images/avatar.svg	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/gin-and-juice-distillery.jpg	AWSALB
GET	https://ginandjuice.shop/resources/images/gin-and-juice-distillery.jpg	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.jpg	AWSALB
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.jpg	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.mp4	AWSALB
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.mp4	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/not-found.svg	AWSALB
GET	https://ginandjuice.shop/resources/images/not-found.svg	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/rating1.png	AWSALB
GET	https://ginandjuice.shop/resources/images/rating1.png	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/rating2.png	AWSALB
GET	https://ginandjuice.shop/resources/images/rating2.png	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/rating3.png	AWSALB
GET	https://ginandjuice.shop/resources/images/rating3.png	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/rating4.png	AWSALB
GET	https://ginandjuice.shop/resources/images/rating4.png	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/rating5.png	AWSALB
GET	https://ginandjuice.shop/resources/images/rating5.png	AWSALBCORS
	https://ginandjuice.shop/resource	

GET	s/images/tracker.gif?searchTerms='+query+'	AWSALB
GET	https://ginandjuice.shop/resources/images/tracker.gif?searchTerms='+query+'	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/angular_1-7-7.js	AWSALB
GET	https://ginandjuice.shop/resources/js/angular_1-7-7.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/deparam.js	AWSALB
GET	https://ginandjuice.shop/resources/js/deparam.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/react-dom.development.js	AWSALB
GET	https://ginandjuice.shop/resources/js/react-dom.development.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/react.development.js	AWSALB
GET	https://ginandjuice.shop/resources/js/react.development.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/searchLogger.js	AWSALB
GET	https://ginandjuice.shop/resources/js/searchLogger.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/stockCheck.js	AWSALB
GET	https://ginandjuice.shop/resources/js/stockCheck.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/subscribeNow.js	AWSALB
GET	https://ginandjuice.shop/resources/js/subscribeNow.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/xmlStockCheckPayload.js	AWSALB
GET	https://ginandjuice.shop/resources/js/xmlStockCheckPayload.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/labheader/css/scanMeHeader.css	AWSALB
GET	https://ginandjuice.shop/resources/labheader/css/scanMeHeader.css	AWSALBCORS
GET	https://ginandjuice.shop/robots.t	AWSALB

	xt	
GET	https://ginandjuice.shop/robots.txt	AWSALBCORS
GET	https://ginandjuice.shop/sitemap.xml	AWSALB
GET	https://ginandjuice.shop/sitemap.xml	AWSALBCORS
GET	https://ginandjuice.shop/upcycling%E2%80%99	AWSALB
GET	https://ginandjuice.shop/upcycling%E2%80%99	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALB
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
	https://ginandjuice.shop/catalog/	

Cookie Without Secure Flag

Hit **88** resources

DESCRIPTION

A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

RECOMMENDED SOLUTION

Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

AFFECTED RESOURCES (88)

Method	URL	Param	Attack Payload (Snippet)
GET	https://ginandjuice.shop	AWSALB	
GET	https://ginandjuice.shop/	AWSALB	
GET	https://ginandjuice.shop/about	AWSALB	
GET	https://ginandjuice.shop/blog	AWSALB	
GET	https://ginandjuice.shop/blog/?back=https%3A%2F%2Fzap.example.com&search=ZAP	AWSALB	

	search=ZAP	
GET	https://ginandjuice.shop/blog/post?postId=1	AWSALB
GET	https://ginandjuice.shop/blog/post?postId=2	AWSALB
GET	https://ginandjuice.shop/blog/post?postId=3	AWSALB
GET	https://ginandjuice.shop/blog/post?postId=4	AWSALB
GET	https://ginandjuice.shop/blog/post?postId=5	AWSALB
GET	https://ginandjuice.shop/blog/post?postId=6	AWSALB
GET	https://ginandjuice.shop/catalog	AWSALB
GET	https://ginandjuice.shop/catalog/cart	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=1	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=10	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=11	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=12	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=13	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=14	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=15	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=16	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=17	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=18	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=2	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=3	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=4	AWSALB

GET	https://ginandjuice.shop/catalog/product?productId=5	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=6	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=7	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=8	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=9	AWSALB
GET	https://ginandjuice.shop/catalog?searchTerm=ZAP	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/1.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/2.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/3.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/4.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/5.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/6.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/1.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/10.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/11.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/12.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/2.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/3.png	AWSALB
	https://ginandjuice.shop/image/sc	

GET	anme/productcatalog/products/4.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/5.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/6.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/7.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/8.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/9.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/batch_1337.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/kettle_still.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/lost_in_a_heyes.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/original_dry_sqli.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/pineapple_edition.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/purple_hat.png	AWSALB
GET	https://ginandjuice.shop/login	AWSALB
GET	https://ginandjuice.shop/my-account	AWSALB
GET	https://ginandjuice.shop/resources/css/labsBlog.css	AWSALB
GET	https://ginandjuice.shop/resources/css/labsEcommerce.css	AWSALB
GET	https://ginandjuice.shop/resources/css/labsScanme.css	AWSALB
GET	https://ginandjuice.shop/resource	AWSALB

	s/footer/js/scanme.js	
GET	https://ginandjuice.shop/resources/images/avatar.svg	AWSALB
GET	https://ginandjuice.shop/resources/images/gin-and-juice-distillery.jpg	AWSALB
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.jpg	AWSALB
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.mp4	AWSALB
GET	https://ginandjuice.shop/resources/images/not-found.svg	AWSALB
GET	https://ginandjuice.shop/resources/images/rating1.png	AWSALB
GET	https://ginandjuice.shop/resources/images/rating2.png	AWSALB
GET	https://ginandjuice.shop/resources/images/rating3.png	AWSALB
GET	https://ginandjuice.shop/resources/images/rating4.png	AWSALB
GET	https://ginandjuice.shop/resources/images/rating5.png	AWSALB
GET	https://ginandjuice.shop/resources/images/tracker.gif?searchTerms='+query+'	AWSALB
GET	https://ginandjuice.shop/resources/js/angular_1-7-7.js	AWSALB
GET	https://ginandjuice.shop/resources/js/deparam.js	AWSALB
GET	https://ginandjuice.shop/resources/js/react-dom.development.js	AWSALB
GET	https://ginandjuice.shop/resources/js/react.development.js	AWSALB
GET	https://ginandjuice.shop/resources/js/searchLogger.js	AWSALB
GET	https://ginandjuice.shop/resources/js/stockCheck.js	AWSALB
GET	https://ginandjuice.shop/resources/js/subscribeNow.js	AWSALB

Cookie with SameSite Attribute None

Hit **89** resources

DESCRIPTION

A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

RECOMMENDED SOLUTION

Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

AFFECTED RESOURCES (89)

Method	URL	Param	Attack Payload (Snippet)
GET	https://ginandjuice.shop	AWSALBCORS	
GET	https://ginandjuice.shop	session	
GET	https://ginandjuice.shop/	AWSALBCORS	
GET	https://ginandjuice.shop/about	AWSALBCORS	
GET	https://ginandjuice.shop/blog	AWSALBCORS	
GET	https://ginandjuice.shop/blog/?back=https%3A%2F%2Fzap.example.com&search=ZAP	AWSALBCORS	
GET	https://ginandjuice.shop/blog/post?postId=1	AWSALBCORS	
GET	https://ginandjuice.shop/blog/post?postId=2	AWSALBCORS	
GET	https://ginandjuice.shop/blog/post?postId=3	AWSALBCORS	
GET	https://ginandjuice.shop/blog/post?postId=4	AWSALBCORS	
GET	https://ginandjuice.shop/blog/post?postId=5	AWSALBCORS	
GET	https://ginandjuice.shop/blog/post?postId=6	AWSALBCORS	
GET	https://ginandjuice.shop/catalog	AWSALBCORS	
GET	https://ginandjuice.shop/catalog/cart	AWSALBCORS	
GET	https://ginandjuice.shop/catalog/product?productId=1	AWSALBCORS	

GET	https://ginandjuice.shop/catalog/product?productId=10	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=11	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=12	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=13	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=14	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=15	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=16	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=17	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=18	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=2	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=3	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=4	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=5	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=6	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=7	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=8	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=9	AWSALBCORS
GET	https://ginandjuice.shop/catalog?searchTerm=ZAP	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/1.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/2.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/3.jpg	AWSALBCORS

	anme/blog/posts/3.jpg	
GET	https://ginandjuice.shop/image/scanme/blog/posts/4.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/5.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/6.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/1.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/10.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/11.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/12.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/2.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/3.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/4.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/5.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/6.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/7.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/8.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/9.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/batch_1337.png	AWSALBCORS

GET	https://ginandjuice.shop/image/scanme/productcatalog/products/kettle_still.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/lost_in_a_heyes.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/original_dry_sqli.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/pineapple_edition.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/purple_hat.png	AWSALBCORS
GET	https://ginandjuice.shop/login	AWSALBCORS
GET	https://ginandjuice.shop/my-account	AWSALBCORS
GET	https://ginandjuice.shop/resources/css/labsBlog.css	AWSALBCORS
GET	https://ginandjuice.shop/resources/css/labsEcommerce.css	AWSALBCORS
GET	https://ginandjuice.shop/resources/css/labsScanme.css	AWSALBCORS
GET	https://ginandjuice.shop/resources/footer/js/scanme.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/avatar.svg	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/gin-and-juice-distillery.jpg	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.jpg	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.mp4	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/not-found.svg	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/rating1.png	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/rating2.png	AWSALBCORS

Cookie without SameSite Attribute

Hit **89** resources

DESCRIPTION

A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

RECOMMENDED SOLUTION

Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

AFFECTED RESOURCES (89)

Method	URL	Param	Attack Payload (Snippet)
GET	https://ginandjuice.shop	AWSALB	
GET	https://ginandjuice.shop/	AWSALB	
GET	https://ginandjuice.shop/about	AWSALB	
GET	https://ginandjuice.shop/blog	AWSALB	
GET	https://ginandjuice.shop/blog/?back=https%3A%2F%2Fzap.example.com&search=ZAP	AWSALB	
GET	https://ginandjuice.shop/blog/post?postId=1	AWSALB	
GET	https://ginandjuice.shop/blog/post?postId=2	AWSALB	
GET	https://ginandjuice.shop/blog/post?postId=3	AWSALB	
GET	https://ginandjuice.shop/blog/post?postId=4	AWSALB	
GET	https://ginandjuice.shop/blog/post?postId=5	AWSALB	
GET	https://ginandjuice.shop/blog/post?postId=6	AWSALB	
GET	https://ginandjuice.shop/catalog	AWSALB	
GET	https://ginandjuice.shop/catalog	TrackingId	
GET	https://ginandjuice.shop/catalog/cart	AWSALB	
GET	https://ginandjuice.shop/catalog/product?productId=1	AWSALB	

GET	https://ginandjuice.shop/catalog/product?productId=10	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=11	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=12	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=13	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=14	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=15	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=16	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=17	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=18	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=2	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=3	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=4	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=5	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=6	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=7	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=8	AWSALB
GET	https://ginandjuice.shop/catalog/product?productId=9	AWSALB
GET	https://ginandjuice.shop/catalog?searchTerm=ZAP	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/1.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/2.jpg	AWSALB
GET	https://ginandjuice.shop/image/sc	

GET	anme/blog/posts/3.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/4.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/5.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/blog/posts/6.jpg	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/1.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/10.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/11.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/12.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/2.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/3.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/4.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/5.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/6.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/7.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/8.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/9.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/batch_1337.png	AWSALB

GET	https://ginandjuice.shop/image/scanme/productcatalog/products/kettle_still.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/lost_in_a_heyes.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/original_dry_sqli.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/pineapple_edition.png	AWSALB
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/purple_hat.png	AWSALB
GET	https://ginandjuice.shop/login	AWSALB
GET	https://ginandjuice.shop/my-account	AWSALB
GET	https://ginandjuice.shop/resources/css/labsBlog.css	AWSALB
GET	https://ginandjuice.shop/resources/css/labsEcommerce.css	AWSALB
GET	https://ginandjuice.shop/resources/css/labsScanme.css	AWSALB
GET	https://ginandjuice.shop/resources/footer/js/scanme.js	AWSALB
GET	https://ginandjuice.shop/resources/images/avatar.svg	AWSALB
GET	https://ginandjuice.shop/resources/images/gin-and-juice-distillery.jpg	AWSALB
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.jpg	AWSALB
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.mp4	AWSALB
GET	https://ginandjuice.shop/resources/images/not-found.svg	AWSALB
GET	https://ginandjuice.shop/resources/images/rating1.png	AWSALB
GET	https://ginandjuice.shop/resources/images/rating2.png	AWSALB

Strict-Transport-Security Header Not Set

Hit **86** resources

DESCRIPTION

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

RECOMMENDED SOLUTION

Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

AFFECTED RESOURCES (86)

Method	URL	Param	Attack Payload (Snippet)
GET	https://ginandjuice.shop	-	
GET	https://ginandjuice.shop/	-	
GET	https://ginandjuice.shop/about	-	
GET	https://ginandjuice.shop/blog	-	
GET	https://ginandjuice.shop/blog/?back=https%3A%2F%2Fzap.example.com&search=ZAP	-	
GET	https://ginandjuice.shop/blog/post?postId=1	-	
GET	https://ginandjuice.shop/blog/post?postId=2	-	
GET	https://ginandjuice.shop/blog/post?postId=3	-	
GET	https://ginandjuice.shop/blog/post?postId=4	-	
GET	https://ginandjuice.shop/blog/post?postId=5	-	
GET	https://ginandjuice.shop/blog/post?postId=6	-	
GET	https://ginandjuice.shop/catalog	-	
GET	https://ginandjuice.shop/catalog/cart	-	
GET	https://ginandjuice.shop/catalog/	-	

	product?productId=1	
GET	https://ginandjuice.shop/catalog/product?productId=10	-
GET	https://ginandjuice.shop/catalog/product?productId=11	-
GET	https://ginandjuice.shop/catalog/product?productId=12	-
GET	https://ginandjuice.shop/catalog/product?productId=13	-
GET	https://ginandjuice.shop/catalog/product?productId=14	-
GET	https://ginandjuice.shop/catalog/product?productId=15	-
GET	https://ginandjuice.shop/catalog/product?productId=16	-
GET	https://ginandjuice.shop/catalog/product?productId=17	-
GET	https://ginandjuice.shop/catalog/product?productId=18	-
GET	https://ginandjuice.shop/catalog/product?productId=2	-
GET	https://ginandjuice.shop/catalog/product?productId=3	-
GET	https://ginandjuice.shop/catalog/product?productId=4	-
GET	https://ginandjuice.shop/catalog/product?productId=5	-
GET	https://ginandjuice.shop/catalog/product?productId=6	-
GET	https://ginandjuice.shop/catalog/product?productId=7	-
GET	https://ginandjuice.shop/catalog/product?productId=8	-
GET	https://ginandjuice.shop/catalog/product?productId=9	-
GET	https://ginandjuice.shop/catalog?searchTerm=ZAP	-
GET	https://ginandjuice.shop/image/scanme/blog/posts/1.jpg	-
GET	https://ginandjuice.shop/image/scanme/blog/posts/2.jpg	-

GET	https://ginandjuice.shop/image/scanme/blog/posts/3.jpg	-
GET	https://ginandjuice.shop/image/scanme/blog/posts/4.jpg	-
GET	https://ginandjuice.shop/image/scanme/blog/posts/5.jpg	-
GET	https://ginandjuice.shop/image/scanme/blog/posts/6.jpg	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/1.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/10.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/11.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/12.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/2.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/3.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/4.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/5.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/6.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/7.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/8.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/9.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/batch_1337.png	-

GET	https://ginandjuice.shop/image/scanme/productcatalog/products/kettle_still.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/lost_in_a_heyes.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/original_dry_sqli.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/pineapple_edition.png	-
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/purple_hat.png	-
GET	https://ginandjuice.shop/login	-
GET	https://ginandjuice.shop/resources/css/labsBlog.css	-
GET	https://ginandjuice.shop/resources/css/labsEcommerce.css	-
GET	https://ginandjuice.shop/resources/css/labsScanme.css	-
GET	https://ginandjuice.shop/resources/footer/js/scanme.js	-
GET	https://ginandjuice.shop/resources/images/avatar.svg	-
GET	https://ginandjuice.shop/resources/images/gin-and-juice-distillery.jpg	-
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.jpg	-
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.mp4	-
GET	https://ginandjuice.shop/resources/images/not-found.svg	-
GET	https://ginandjuice.shop/resources/images/rating1.png	-

X-Content-Type-Options Header Missing

Hit **81** resources

DESCRIPTION

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

RECOMMENDED SOLUTION

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.
If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/ web server to not perform MIME-sniffing.

AFFECTED RESOURCES (81)

Method	URL	Param	Attack Payload (Snippet)
GET	https://ginandjuice.shop	x-content-type-options	
GET	https://ginandjuice.shop/	x-content-type-options	
GET	https://ginandjuice.shop/about	x-content-type-options	
GET	https://ginandjuice.shop/blog	x-content-type-options	
GET	https://ginandjuice.shop/blog/?back=https%3A%2F%2Fzap.example.com&search=ZAP	x-content-type-options	
GET	https://ginandjuice.shop/blog/post?postId=1	x-content-type-options	
GET	https://ginandjuice.shop/blog/post?postId=2	x-content-type-options	
GET	https://ginandjuice.shop/blog/post?postId=3	x-content-type-options	
GET	https://ginandjuice.shop/blog/post?postId=4	x-content-type-options	
GET	https://ginandjuice.shop/blog/post?postId=5	x-content-type-options	
GET	https://ginandjuice.shop/blog/post?postId=6	x-content-type-options	
GET	https://ginandjuice.shop/catalog	x-content-type-options	

GET	https://ginandjuice.shop/catalog/cart	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=1	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=10	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=11	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=12	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=13	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=14	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=15	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=16	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=17	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=18	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=2	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=3	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=4	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=5	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=6	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=7	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=8	x-content-type-options
GET	https://ginandjuice.shop/catalog/product?productId=9	x-content-type-options
GET	https://ginandjuice.shop/catalog?searchTerm=ZAP	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/blog/posts/1.jpg	x-content-type-options

GET	https://ginandjuice.shop/image/scanme/blog/posts/2.jpg	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/blog/posts/3.jpg	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/blog/posts/4.jpg	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/blog/posts/5.jpg	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/blog/posts/6.jpg	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/1.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/10.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/11.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/12.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/2.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/3.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/4.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/5.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/6.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/7.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/8.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/9.png	x-content-type-options

	y	
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/batch_1337.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/kettle_still.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/lost_in_a_heyes.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/original_dry_sqli.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/pineapple_edition.png	x-content-type-options
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/purple_hat.png	x-content-type-options
GET	https://ginandjuice.shop/login	x-content-type-options
GET	https://ginandjuice.shop/resources/css/labsBlog.css	x-content-type-options
GET	https://ginandjuice.shop/resources/css/labsEcommerce.css	x-content-type-options
GET	https://ginandjuice.shop/resources/css/labsScanme.css	x-content-type-options
GET	https://ginandjuice.shop/resources/footer/js/scanme.js	x-content-type-options
GET	https://ginandjuice.shop/resources/images/avatar.svg	x-content-type-options
GET	https://ginandjuice.shop/resources/images/gin-and-juice-distillery.jpg	x-content-type-options
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.jpg	x-content-type-options

Information Disclosure - Suspicious Comments

Hit **4** resources

DESCRIPTION

The response appears to contain suspicious comments which may help an attacker.

RECOMMENDED SOLUTION

Modern Web Application

Hit **36** resources

DESCRIPTION

The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

RECOMMENDED SOLUTION

This is an informational alert and so no changes are required.

AFFECTED RESOURCES (36)

Method	URL	Param	Attack Payload (Snippet)
GET	https://ginandjuice.shop	-	
GET	https://ginandjuice.shop/	-	
GET	https://ginandjuice.shop/about	-	
GET	https://ginandjuice.shop/blog	-	
GET	https://ginandjuice.shop/blog/?back=https%3A%2F%2Fzap.example.com&search=ZAP	-	
GET	https://ginandjuice.shop/blog/post?postId=1	-	
GET	https://ginandjuice.shop/blog/post?postId=2	-	
GET	https://ginandjuice.shop/blog/post?postId=3	-	
GET	https://ginandjuice.shop/blog/post?postId=4	-	
GET	https://ginandjuice.shop/blog/post?postId=5	-	
GET	https://ginandjuice.shop/blog/post?postId=6	-	
GET	https://ginandjuice.shop/catalog	-	
GET	https://ginandjuice.shop/catalog/cart	-	
GET	https://ginandjuice.shop/catalog/product?productId=1	-	

GET	https://ginandjuice.shop/catalog/product?productId=10	-
GET	https://ginandjuice.shop/catalog/product?productId=11	-
GET	https://ginandjuice.shop/catalog/product?productId=12	-
GET	https://ginandjuice.shop/catalog/product?productId=13	-
GET	https://ginandjuice.shop/catalog/product?productId=14	-
GET	https://ginandjuice.shop/catalog/product?productId=15	-
GET	https://ginandjuice.shop/catalog/product?productId=16	-
GET	https://ginandjuice.shop/catalog/product?productId=17	-
GET	https://ginandjuice.shop/catalog/product?productId=18	-
GET	https://ginandjuice.shop/catalog/product?productId=2	-
GET	https://ginandjuice.shop/catalog/product?productId=3	-
GET	https://ginandjuice.shop/catalog/product?productId=4	-
GET	https://ginandjuice.shop/catalog/product?productId=5	-
GET	https://ginandjuice.shop/catalog/product?productId=6	-
GET	https://ginandjuice.shop/catalog/product?productId=7	-
GET	https://ginandjuice.shop/catalog/product?productId=8	-
GET	https://ginandjuice.shop/catalog/product?productId=9	-
GET	https://ginandjuice.shop/catalog?searchTerm=ZAP	-
GET	https://ginandjuice.shop/login	-
GET	https://ginandjuice.shop/robots.txt	-
GET	https://ginandjuice.shop/sitemap.xml	-

GET	https://ginandjuice.shop/upcycli n%E2%80%99	-

Re-examine Cache-control Directives

Hit **33** resources

DESCRIPTION

The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

RECOMMENDED SOLUTION

For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

AFFECTED RESOURCES (33)

Method	URL	Param	Attack Payload (Snippet)
GET	https://ginandjuice.shop	cache-control	
GET	https://ginandjuice.shop/	cache-control	
GET	https://ginandjuice.shop/about	cache-control	
GET	https://ginandjuice.shop/blog	cache-control	
GET	https://ginandjuice.shop/blog/?back=https%3A%2F%2Fzap.example.com&search=ZAP	cache-control	
GET	https://ginandjuice.shop/blog/post?postId=1	cache-control	
GET	https://ginandjuice.shop/blog/post?postId=2	cache-control	
GET	https://ginandjuice.shop/blog/post?postId=3	cache-control	
GET	https://ginandjuice.shop/blog/post?postId=4	cache-control	
GET	https://ginandjuice.shop/blog/post?postId=5	cache-control	
GET	https://ginandjuice.shop/blog/post?postId=6	cache-control	

GET	https://ginandjuice.shop/catalog	cache-control
GET	https://ginandjuice.shop/catalog/cart	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=1	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=10	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=11	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=12	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=13	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=14	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=15	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=16	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=17	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=18	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=2	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=3	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=4	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=5	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=6	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=7	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=8	cache-control
GET	https://ginandjuice.shop/catalog/product?productId=9	cache-control
GET	https://ginandjuice.shop/catalog?searchTerm=ZAP	cache-control

Session Management Response Identified

Hit **125** resources

DESCRIPTION

The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

RECOMMENDED SOLUTION

This is an informational alert rather than a vulnerability and so there is nothing to fix.

AFFECTED RESOURCES (125)

Method	URL	Param	Attack Payload (Snippet)
GET	https://ginandjuice.shop	session	
GET	https://ginandjuice.shop	session	
GET	https://ginandjuice.shop/	AWSALBCORS	
GET	https://ginandjuice.shop/about	AWSALBCORS	
GET	https://ginandjuice.shop/blog	AWSALBCORS	
GET	https://ginandjuice.shop/blog/?back=https%3A%2F%2Fzap.example.com&search=ZAP	AWSALBCORS	
GET	https://ginandjuice.shop/blog/post?postId=1	AWSALBCORS	
GET	https://ginandjuice.shop/blog/post?postId=2	AWSALBCORS	
GET	https://ginandjuice.shop/blog/post?postId=3	AWSALBCORS	
GET	https://ginandjuice.shop/blog/post?postId=4	AWSALBCORS	
GET	https://ginandjuice.shop/blog/post?postId=5	AWSALBCORS	
GET	https://ginandjuice.shop/blog/post?postId=6	AWSALBCORS	
GET	https://ginandjuice.shop/catalog	TrackingId	
GET	https://ginandjuice.shop/catalog/	AWSALBCORS	

	cart	
GET	https://ginandjuice.shop/catalog/product?productId=1	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=10	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=11	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=12	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=13	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=14	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=15	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=16	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=17	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=18	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=2	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=3	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=4	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=5	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=6	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=7	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=8	AWSALBCORS
GET	https://ginandjuice.shop/catalog/product?productId=9	AWSALBCORS
GET	https://ginandjuice.shop/catalog?searchTerm=ZAP	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/1.jpg	AWSALBCORS
	https://ginandjuice.shop/image/sc	

GET	https://ginandjuice.shop/image/scanme/blog/posts/2.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/3.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/4.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/5.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/blog/posts/6.jpg	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/1.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/10.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/11.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/12.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/2.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/3.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/4.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/5.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/6.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/7.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/8.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/9.png	AWSALBCORS

GET	https://ginandjuice.shop/image/scanme/productcatalog/products/batch_1337.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/kettle_still.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/lost_in_a_heyes.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/original_dry_sqli.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/pineapple_edition.png	AWSALBCORS
GET	https://ginandjuice.shop/image/scanme/productcatalog/products/purple_hat.png	AWSALBCORS
GET	https://ginandjuice.shop/login	AWSALBCORS
GET	https://ginandjuice.shop/my-account	AWSALBCORS
GET	https://ginandjuice.shop/resources/css/labsBlog.css	AWSALBCORS
GET	https://ginandjuice.shop/resources/css/labsEcommerce.css	AWSALBCORS
GET	https://ginandjuice.shop/resources/css/labsScanme.css	AWSALBCORS
GET	https://ginandjuice.shop/resources/footer/js/scanme.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/avatar.svg	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/gin-and-juice-distillery.jpg	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.jpg	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/gin-and-juice-team.mp4	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/not-found.svg	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/rating1.png	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/rating2.png	AWSALBCORS

GET	https://ginandjuice.shop/resources/images/rating3.png	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/rating4.png	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/rating5.png	AWSALBCORS
GET	https://ginandjuice.shop/resources/images/tracker.gif?searchTerms='+query+'	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/angular_1-7-7.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/deparam.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/react-dom.development.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/react.development.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/searchLogger.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/stockCheck.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/subscribeNow.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/js/xmlStockCheckPayload.js	AWSALBCORS
GET	https://ginandjuice.shop/resources/labheader/css/scanMeHeader.css	AWSALBCORS
GET	https://ginandjuice.shop/robots.txt	AWSALBCORS
GET	https://ginandjuice.shop/sitemap.xml	AWSALBCORS
GET	https://ginandjuice.shop/upcycli n%E2%80%99	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS

POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/cart	AWSALBCORS
POST	https://ginandjuice.shop/catalog/	AWSALBCORS

User Controllable HTML Element Attribute (Potential XSS)

Hit **16** resources

DESCRIPTION

This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.

RECOMMENDED SOLUTION

Validate all input and sanitize output it before writing to any HTML attributes.

AFFECTED RESOURCES (16)

Method	URL	Param	Attack Payload (Snippet)
GET	https://ginandjuice.shop/blog/?back=https%3A%2F%2Fzap.example.com&search=ZAP	search	
GET	https://ginandjuice.shop/catalog/product?productId=10	productId	
GET	https://ginandjuice.shop/catalog/product?productId=10	productId	
GET	https://ginandjuice.shop/catalog/product?productId=11	productId	
GET	https://ginandjuice.shop/catalog/product?productId=11	productId	
GET	https://ginandjuice.shop/catalog/product?productId=12	productId	
GET	https://ginandjuice.shop/catalog/product?productId=12	productId	
GET	https://ginandjuice.shop/catalog/product?productId=13	productId	
GET	https://ginandjuice.shop/catalog/product?productId=13	productId	
GET	https://ginandjuice.shop/catalog/product?productId=14	productId	
GET	https://ginandjuice.shop/catalog/product?productId=14	productId	
GET	https://ginandjuice.shop/catalog/product?productId=15	productId	
GET	https://ginandjuice.shop/catalog/product?productId=15	productId	
GET	https://ginandjuice.shop/catalog/product?productId=16	productId	
GET	https://ginandjuice.shop/catalog/product?productId=17	productId	
GET	https://ginandjuice.shop/catalog/product?productId=18	productId	

END OF REPORT