ZAP Scanning Report

Site: https://liborate-staging.vercel.app

Generated on Sun, 10 Aug 2025 09:23:36

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	5
Low	2
Informational	11
False Positives:	0

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Alerts

Name	Risk Level	Number of Instances
CSP: Failure to Define Directive with No Fallback	Medium	3
CSP: script-src unsafe-eval	Medium	3
CSP: script-src unsafe-inline	Medium	3
CSP: style-src unsafe-inline	Medium	3
Cross-Domain Misconfiguration	Medium	11
Insufficient Site Isolation Against Spectre Vulnerability	Low	2
Permissions Policy Header Not Set	Low	10
Base64 Disclosure	Informational	1
Information Disclosure - Suspicious Comments	Informational	4
Modern Web Application	Informational	3
Re-examine Cache-control Directives	Informational	1
Retrieved from Cache	Informational	11
Sec-Fetch-Dest Header is Missing	Informational	2
Sec-Fetch-Mode Header is Missing	Informational	2
Sec-Fetch-Site Header is Missing	Informational	2
Sec-Fetch-User Header is Missing	Informational	2
Storable and Cacheable Content	Informational	7

Storable but Non-Cacheable Content	Informational	4

Alert Detail

Medium	**CSP: Failure to Define Directive with No Fallback**
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding them is the same as allowing anything.
URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' data:; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; media-src 'self' www.youtube.com; frame-src 'self' https://www.youtube.com *.youtube.com https://www.youtube.com/embed/ *.youtube.com/embed/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google-analytics.com/ https://www.youtube.com/ https://s.ytimg.com; object-src 'self'; child-src https://www.youtube.com/ https://s.ytimg.com
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://liborate-staging.vercel.app/robots.txt
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' data:; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; media-src 'self' www.youtube.com; frame-src 'self' https://www.youtube.com *.youtube.com https://www.youtube.com/embed/ *.youtube.com/embed/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google-analytics.com/ https://www.youtube.com/ https://s.ytimg.com; object-src 'self'; child-src https://www.youtube.com/ https://s.ytimg.com
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://liborate-staging.vercel.app/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' data:; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; media-src 'self' www.youtube.com; frame-src 'self' https://www.youtube.com *.youtube.com https://www.youtube.com/embed/ *.youtube.com/embed/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google-analytics.com/ https://www.youtube.com/ https://s.ytimg.com; object-src 'self'; child-src https://www.youtube.com/ https://s.ytimg.com
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CWE Id	693
WASC Id	15
Plugin Id	10055

Medium **CSP: script-src unsafe-eval**

Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' data:; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; media-src 'self' www.youtube.com; frame-src 'self' https://www.youtube.com *.youtube.com https://www.youtube.com/embed/ *.youtube.com/embed/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google-analytics.com/ https://www.youtube.com/ https://s.ytimg.com; object-src 'self'; child-src https://www.youtube.com/ https://s.ytimg.com
Other Info	script-src includes unsafe-eval.
URL	https://liborate-staging.vercel.app/robots.txt
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' data:; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; media-src 'self' www.youtube.com; frame-src 'self' https://www.youtube.com *.youtube.com https://www.youtube.com/embed/ *.youtube.com/embed/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google-analytics.com/ https://www.youtube.com/ https://s.ytimg.com; object-src 'self'; child-src https://www.youtube.com/ https://s.ytimg.com
Other Info	script-src includes unsafe-eval.
URL	https://liborate-staging.vercel.app/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' data:; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; media-src 'self' www.youtube.com; frame-src 'self' https://www.youtube.com *.youtube.com https://www.youtube.com/embed/ *.youtube.com/embed/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google-analytics.com/ https://www.youtube.com/ https://s.ytimg.com; object-src 'self'; child-src https://www.youtube.com/ https://s.ytimg.com
Other Info	script-src includes unsafe-eval.
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp

	https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium **CSP: script-src unsafe-inline**

Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' data:; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; media-src 'self' www.youtube.com; frame-src 'self' https://www.youtube.com *.youtube.com https://www.youtube.com/embed/ *.youtube.com/embed/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google-analytics.com/ https://www.youtube.com/ https://s.ytimg.com; object-src 'self'; child-src https://www.youtube.com/ https://s.ytimg.com
Other Info	script-src includes unsafe-inline.
URL	https://liborate-staging.vercel.app/robots.txt
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' data:; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; media-src 'self' www.youtube.com; frame-src 'self' https://www.youtube.com *.youtube.com https://www.youtube.com/embed/ *.youtube.com/embed/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google-analytics.com/ https://www.youtube.com/ https://s.ytimg.com; object-src 'self'; child-src https://www.youtube.com/ https://s.ytimg.com
Other Info	script-src includes unsafe-inline.
URL	https://liborate-staging.vercel.app/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' data:; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; media-src 'self' www.youtube.com; frame-src 'self' https://www.youtube.com *.youtube.com https://www.youtube.com/embed/ *.youtube.com/embed/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google-analytics.com/ https://www.youtube.com/ https://s.ytimg.com; object-src 'self'; child-src https://www.youtube.com/ https://s.ytimg.com
Other Info	script-src includes unsafe-inline.
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/

	https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: style-src unsafe-inline**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' data:; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; media-src 'self' www.youtube.com; frame-src 'self' https://www.youtube.com *.youtube.com https://www.youtube.com/embed/ *.youtube.com/embed/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google-analytics.com/ https://www.youtube.com/ https://s.ytimg.com; object-src 'self'; child-src https://www.youtube.com/ https://s.ytimg.com
Other Info	style-src includes unsafe-inline.
URL	https://liborate-staging.vercel.app/robots.txt
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' data:; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; media-src 'self' www.youtube.com; frame-src 'self' https://www.youtube.com *.youtube.com https://www.youtube.com/embed/ *.youtube.com/embed/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google-analytics.com/ https://www.youtube.com/ https://s.ytimg.com; object-src 'self'; child-src https://www.youtube.com/ https://s.ytimg.com
Other Info	style-src includes unsafe-inline.
URL	https://liborate-staging.vercel.app/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' data:; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; media-src 'self' www.youtube.com; frame-src 'self' https://www.youtube.com *.youtube.com https://www.youtube.com/embed/ *.youtube.com/embed/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google-analytics.com/ https://www.youtube.com/ https://s.ytimg.com; object-src 'self'; child-src https://www.youtube.com/ https://s.ytimg.com
Other Info	style-src includes unsafe-inline.
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy

	https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://liborate-staging.vercel.app/_next/static/chunks/454-224a6a4c9da42732.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://liborate-staging.vercel.app/_next/static/chunks/684-911a23eaa1d0a90c.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://liborate-staging.vercel.app/_next/static/chunks/app/page-87ab5a72c4762152.js
Method	GET
Parameter	
Attack	

Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://liborate-staging.vercel.app/_next/static/chunks/main-app-d9794b1200c643e4.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://liborate-staging.vercel.app/_next/static/chunks/polyfills-42372ed130431b0a.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://liborate-staging.vercel.app/_next/static/chunks/webpack-06156908721125d6.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://liborate-staging.vercel.app/_next/static/css/79704f59dd404b18.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an

	attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://liborate-staging.vercel.app/favicon.ico
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://liborate-staging.vercel.app/robots.txt
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://liborate-staging.vercel.app/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	11
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Low **Insufficient Site Isolation Against Spectre Vulnerability**

Description	Cross-Origin-Embedder-Policy header is a response header that prevents a document from loading any cross-origin resources that don't explicitly grant the document permission (using CORP or CORS).
URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	Cross-Origin-Embedder-Policy
Attack	
Evidence	
Other Info	
URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	Cross-Origin-Opener-Policy
Attack	
Evidence	
Other Info	
Instances	2
Solution	Ensure that the application/web server sets the Cross-Origin-Embedder-Policy header appropriately, and that it sets the Cross-Origin-Embedder-Policy header to 'require-corp' for documents. If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Embedder-Policy header (https://caniuse.com/mdn-http_headers_cross-origin-embedder-policy).
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cross-Origin-Embedder-Policy
CWE Id	693
WASC Id	14
Plugin Id	90004

Low	**Permissions Policy Header Not Set**
Description	Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://liborate-staging.vercel.app/_next/static/chunks/454-224a6a4c9da42732.js
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://liborate-staging.vercel.app/_next/static/chunks/4bd1b696-5e9fb803a7b3b4fe.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://liborate-staging.vercel.app/_next/static/chunks/684-911a23eaa1d0a90c.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://liborate-staging.vercel.app/_next/static/chunks/app/page-87ab5a72c4762152.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://liborate-staging.vercel.app/_next/static/chunks/main-app-d9794b1200c643e4.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://liborate-staging.vercel.app/_next/static/chunks/polyfills-42372ed130431b0a.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://liborate-staging.vercel.app/_next/static/chunks/webpack-06156908721125d6.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://liborate-staging.vercel.app/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://liborate-staging.vercel.app/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	10
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy https://developer.chrome.com/blog/feature-policy/ https://scotthelme.co.uk/a-new-security-header-feature-policy/ https://w3c.github.io/webappsec-feature-policy/ https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	693
WASC Id	15
Plugin Id	10063

Informational	Base64 Disclosure
Description	Base64 encoded data was disclosed by the application/web server. Note: in the interests of performance not all base64 strings in the response were analyzed individually, the entire response should be looked at by the analyst/security team/developer(s).
URL	https://liborate-staging.vercel.app/_next/static/chunks/webpack-06156908721125d6.js
Method	GET
Parameter	
Attack	
Evidence	dpl_Gu1GMHuyutjj3MR8bYvNd2YjrdBd
Other Info	v□□F0{□□□□□□□m□□wf#□□]
Instances	1
Solution	Manually confirm that the Base64 data does not leak sensitive information, and that the data cannot be aggregated/used to exploit other vulnerabilities.
Reference	https://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	319
WASC Id	13
Plugin Id	10094

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.

URL	https://liborate-staging.vercel.app/_next/static/chunks/454-224a6a4c9da42732.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//localhost:3000/api/auth");e&&!e.startsWith("http")&&(e=`https://${e}`);let n=new URL(null!=(t=e)?t:r),o="/"===n.pathname?r.pa", see evidence field for the suspicious comment/snippet.
URL	https://liborate-staging.vercel.app/_next/static/chunks/4bd1b696-5e9fb803a7b3b4fe.js
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//react.dev/errors/"+e;if(1<arguments.length){n+="?args[]="+encodeURIComponent(arguments[1]);for(var t=2;t<arguments.length;t++)", see evidence field for the suspicious comment/snippet.
URL	https://liborate-staging.vercel.app/_next/static/chunks/684-911a23eaa1d0a90c.js
Method	GET
Parameter	
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in likely comment: "//nextjs.org/docs/app/api-reference/functions/use-search-params#updating-searchparams")}}class s extends URLSearchParams{append(", see evidence field for the suspicious comment/snippet.
URL	https://liborate-staging.vercel.app/_next/static/chunks/polyfills-42372ed130431b0a.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//github.com/zloirock/core-js/blob/v3.38.1/LICENSE",source:"https://github.com/zloirock/core-js"})}),nt=function(t,e){return rt[", see evidence field for the suspicious comment/snippet.
Instances	4
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Informational	**Modern Web Application**
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.

URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	
Attack	
Evidence	<script src="/_next/static/chunks/4bd1b696-5e9fb803a7b3b4fe.js" async=""></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://liborate-staging.vercel.app/robots.txt
Method	GET
Parameter	
Attack	
Evidence	<script src="/_next/static/chunks/4bd1b696-5e9fb803a7b3b4fe.js" async=""></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://liborate-staging.vercel.app/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	<script src="/_next/static/chunks/4bd1b696-5e9fb803a7b3b4fe.js" async=""></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	3
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational **Re-examine Cache-control Directives**

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.
URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=0, must-revalidate
Other Info	
Instances	1
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".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching

	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational **Retrieved from Cache**

Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	
Attack	
Evidence	Age: 582
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://liborate-staging.vercel.app/_next/static/chunks/454-224a6a4c9da42732.js
Method	GET
Parameter	
Attack	
Evidence	Age: 0
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://liborate-staging.vercel.app/_next/static/chunks/684-911a23eaa1d0a90c.js
Method	GET
Parameter	
Attack	
Evidence	Age: 0
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://liborate-staging.vercel.app/_next/static/chunks/app/page-87ab5a72c4762152.js
Method	GET
Parameter	
Attack	
Evidence	Age: 0
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://liborate-staging.vercel.app/_next/static/chunks/main-app-d9794b1200c643e4.js
Method	GET
Parameter	
Attack	
Evidence	Age: 0

Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://liborate-staging.vercel.app/_next/static/chunks/polyfills-42372ed130431b0a.js
Method	GET
Parameter	
Attack	
Evidence	Age: 0
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://liborate-staging.vercel.app/_next/static/chunks/webpack-06156908721125d6.js
Method	GET
Parameter	
Attack	
Evidence	Age: 0
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://liborate-staging.vercel.app/_next/static/css/79704f59dd404b18.css
Method	GET
Parameter	
Attack	
Evidence	Age: 0
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://liborate-staging.vercel.app/favicon.ico
Method	GET
Parameter	
Attack	
Evidence	Age: 346
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://liborate-staging.vercel.app/robots.txt
Method	GET
Parameter	
Attack	
Evidence	Age: 0
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://liborate-staging.vercel.app/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	Age: 0
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	11

Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	525
WASC Id	
Plugin Id	10050

Informational **Sec-Fetch-Dest Header is Missing**

Description	Specifies how and where the data would be used. For instance, if the value is audio, then the requested resource must be audio data and not any other type of resource.
URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	Sec-Fetch-Dest
Attack	
Evidence	
Other Info	
URL	https://liborate-staging.vercel.app/robots.txt
Method	GET
Parameter	Sec-Fetch-Dest
Attack	
Evidence	
Other Info	
Instances	2
Solution	Ensure that Sec-Fetch-Dest header is included in request headers.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-Dest
CWE Id	352
WASC Id	9
Plugin Id	90005

Informational **Sec-Fetch-Mode Header is Missing**

Description	Allows to differentiate between requests for navigating between HTML pages and requests for loading resources like images, audio etc.
URL	https://liborate-staging.vercel.app/
Method	GET

Parameter	Sec-Fetch-Mode
Attack	
Evidence	
Other Info	
URL	https://liborate-staging.vercel.app/robots.txt
Method	GET
Parameter	Sec-Fetch-Mode
Attack	
Evidence	
Other Info	
Instances	2
Solution	Ensure that Sec-Fetch-Mode header is included in request headers.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-Mode
CWE Id	352
WASC Id	9
Plugin Id	90005

Informational	Sec-Fetch-Site Header is Missing
Description	Specifies the relationship between request initiator's origin and target's origin.
URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	Sec-Fetch-Site
Attack	
Evidence	
Other Info	
URL	https://liborate-staging.vercel.app/robots.txt
Method	GET
Parameter	Sec-Fetch-Site
Attack	
Evidence	
Other Info	
Instances	2
Solution	Ensure that Sec-Fetch-Site header is included in request headers.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-Site
CWE Id	352
WASC Id	9
Plugin Id	90005

Informational	Sec-Fetch-User Header is Missing
Description	Specifies if a navigation request was initiated by a user.
URL	https://liborate-staging.vercel.app/

Method	GET
Parameter	Sec-Fetch-User
Attack	
Evidence	
Other Info	
URL	https://liborate-staging.vercel.app/robots.txt
Method	GET
Parameter	Sec-Fetch-User
Attack	
Evidence	
Other Info	
Instances	2
Solution	Ensure that Sec-Fetch-User header is included in user initiated requests.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-User
CWE Id	352
WASC Id	9
Plugin Id	90005

Informational	Storable and Cacheable Content
Description	The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://liborate-staging.vercel.app/_next/static/chunks/454-224a6a4c9da42732.js
Method	GET
Parameter	
Attack	
Evidence	max-age=31536000
Other Info	
URL	https://liborate-staging.vercel.app/_next/static/chunks/684-911a23eaa1d0a90c.js
Method	GET
Parameter	
Attack	
Evidence	max-age=31536000
Other Info	
URL	https://liborate-staging.vercel.app/_next/static/chunks/app/page-87ab5a72c4762152.js
Method	GET
Parameter	

Attack	
Evidence	max-age=31536000
Other Info	
URL	https://liborate-staging.vercel.app/_next/static/chunks/main-app-d9794b1200c643e4.js
Method	GET
Parameter	
Attack	
Evidence	max-age=31536000
Other Info	
URL	https://liborate-staging.vercel.app/_next/static/chunks/polyfills-42372ed130431b0a.js
Method	GET
Parameter	
Attack	
Evidence	max-age=31536000
Other Info	
URL	https://liborate-staging.vercel.app/_next/static/chunks/webpack-06156908721125d6.js
Method	GET
Parameter	
Attack	
Evidence	max-age=31536000
Other Info	
URL	https://liborate-staging.vercel.app/_next/static/css/79704f59dd404b18.css
Method	GET
Parameter	
Attack	
Evidence	max-age=31536000
Other Info	
Instances	7
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524

WASC Id	13
Plugin Id	10049

Informational	Storable but Non-Cacheable Content
Description	The response contents are storable by caching components such as proxy servers, but will not be retrieved directly from the cache, without validating the request upstream, in response to similar requests from other users.
URL	https://liborate-staging.vercel.app/
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
URL	https://liborate-staging.vercel.app/favicon.ico
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
URL	https://liborate-staging.vercel.app/robots.txt
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
URL	https://liborate-staging.vercel.app/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
Instances	4
Solution	
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049

Sequence Details

With the associated active scan results.