ZAP by Checkmarx Scanning Report

Sites: http://r11.o.lencr.org http://r10.o.lencr.org https://hariyoilam.shop

Generated on Sun, 1 Dec 2024 12:26:52

ZAP Version: 2.15.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	5
Low	7
Informational	4

Alerts

Name	Risk Level	Number of Instances
PII Disclosure	High	5
Absence of Anti-CSRF Tokens	Medium	2
CSP: Wildcard Directive	Medium	9
CSP: script-src unsafe-inline	Medium	9
CSP: style-src unsafe-inline	Medium	9
Missing Anti-clickjacking Header	Medium	5
Cookie No HttpOnly Flag	Low	2
Cookie without SameSite Attribute	Low	3
Cross-Domain JavaScript Source File Inclusion	Low	8
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	15
Strict-Transport-Security Header Not Set	Low	32
Timestamp Disclosure - Unix	Low	12
X-Content-Type-Options Header Missing	Low	27
Information Disclosure - Suspicious Comments	Informational	24
Modern Web Application	Informational	7
Re-examine Cache-control Directives	Informational	3
Session Management Response Identified	Informational	5

Alert Detail

High	PII Disclosure
Description	The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	4242424242424242
Other Info	Credit Card Type detected: Visa Bank Identification Number: 424242 Brand: VISA Category: Issuer:
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	
Evidence	4242424242424242
Other Info	Credit Card Type detected: Visa Bank Identification Number: 424242 Brand: VISA Category: Issuer:
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	4242424242424242
Other Info	Credit Card Type detected: Visa Bank Identification Number: 424242 Brand: VISA Category: Issuer:
URL	https://hariyoilam.shop/?wc-ajax=update_order_review
Method	POST
Attack	
Evidence	4242424242424242
Other Info	Credit Card Type detected: Visa Bank Identification Number: 424242 Brand: VISA Category: Issuer:
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	4242424242424242
Other Info	Credit Card Type detected: Visa Bank Identification Number: 424242 Brand: VISA Category: Issuer:
Instances	5
Solution	Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.
Reference	
CWE Id	359
WASC Id	13
Plugin Id	10062

Medium	Absence of Anti-CSRF Tokens
	No Anti-CSRF tokens were found in a HTML submission form.

Description	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.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	<form class="cart" action="https://hariyoilam.shop/product/wheat-from-organic-farms/" method="post" enctype='multipart/form-data'>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "quantity_674ca86827674"].
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	<form action="https://hariyoilam.shop/wp-comments-post.php" method="post" id="commentform" class="comment-form">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 2: "author" "comment_parent" "comment_post_ID" "email" "submit" "wp-comment-cookies-consent"].
Instances	2
	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.

Solution	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.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	**CSP: Wildcard Directive**
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://hariyoilam.shop/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://hariyoilam.shop/about/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://hariyoilam.shop/my-account
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://hariyoilam.shop/my-account/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/

Method	POST
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
Instances	9
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://hariyoilam.shop/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://hariyoilam.shop/about/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	

Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://hariyoilam.shop/my-account
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://hariyoilam.shop/my-account/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
Instances	9
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://hariyoilam.shop/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://hariyoilam.shop/about/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://hariyoilam.shop/my-account
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://hariyoilam.shop/my-account/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET

Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
Instances	9
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	**Missing Anti-clickjacking Header**
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://hariyoilam.shop/about/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	

Evidence	
Other Info	
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	
Other Info	
Instances	5
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Low	**Cookie No HttpOnly Flag**
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.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	set-cookie: woocommerce_cart_hash
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	set-cookie: woocommerce_items_in_cart
Other Info	
Instances	2
Solution	Ensure that the HttpOnly flag is set for all cookies.

Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	**Cookie without SameSite Attribute**
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.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	set-cookie: woocommerce_cart_hash
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	set-cookie: woocommerce_items_in_cart
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	set-cookie: wp_woocommerce_session_b32934bef65fc6bdf351776efaf1c8dd
Other Info	
Instances	3
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	<script src="https://js.stripe.com/v3/?ver=1.10.0" id="cpsw-stripe-external-js"></script>
Other Info	
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	

Evidence	<script src="https://js.stripe.com/v3/?ver=3.0" id="stripe-js"></script>
Other Info	
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	
Evidence	<script src="https://js.stripe.com/v3/?ver=1.10.0" id="cpsw-stripe-external-js"></script>
Other Info	
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	
Evidence	<script src="https://js.stripe.com/v3/?ver=3.0" id="stripe-js"></script>
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	<script src="https://js.stripe.com/v3/?ver=1.10.0" id="cpsw-stripe-external-js"></script>
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	<script src="https://js.stripe.com/v3/?ver=3.0" id="stripe-js"></script>
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	<script src="https://js.stripe.com/v3/?ver=1.10.0" id="cpsw-stripe-external-js"></script>
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	<script src="https://js.stripe.com/v3/?ver=3.0" id="stripe-js"></script>
Other Info	
Instances	8
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829

WASC Id	15
Plugin Id	10017

Low	**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	https://hariyoilam.shop/
Method	GET
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/about/
Method	GET
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/my-account
Method	GET
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/my-account/
Method	GET
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/

Method	GET
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/wp-json/wc/store/v1/products/collection-data?min_price=&max_price=&calculate_price_range=true&_locale=user
Method	GET
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/wp-json/wc/store/v1?_locale=user
Method	GET
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/?wc-ajax=get_refreshed_fragments
Method	POST
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/?wc-ajax=update_order_review
Method	POST
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/?wc-ajax=wc_stripe_get_cart_details
Method	POST
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/?wc-ajax=wc_stripe_save_appearance
Method	POST

Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	x-powered-by: PHP/8.2.22
Other Info	
Instances	15
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037

Low	**Strict-Transport-Security Header Not Set**
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.
URL	https://hariyoilam.shop/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/about/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	

Evidence	
Other Info	
URL	https://hariyoilam.shop/my-account/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/elementor/assets/css/conditionals/dialog.min.css?ver=3.25.7
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/elementor/assets/css/conditionals/lightbox.min.css?ver=3.25.7
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/elementor/assets/js/lightbox.01a419d1fcdd47a75a77.bundle.min.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/elementor/assets/lib/dialog/dialog.min.js?ver=4.9.3
Method	GET

Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/elementor/assets/lib/jquery-numerator/jquery-numerator.min.js?ver=0.2.1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/elementor/assets/lib/share-link/share-link.min.js?ver=3.25.7
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/css/photoswipe/default-skin/default-skin.min.css?ver=9.4.1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/css/photoswipe/photoswipe.min.css?ver=9.4.1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/fonts/WooCommerce.woff
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/flexslider/jquery.flexslider.min.js?ver=2.7.2-wc.9.4.1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/frontend/cart.min.js?ver=9.4.1

Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/frontend/single-product.min.js?ver=9.4.1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/photoswipe/photoswipe-ui-default.min.js?ver=4.1.1-wc.9.4.1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/photoswipe/photoswipe.min.js?ver=4.1.1-wc.9.4.1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/zoom/jquery.zoom.min.js?ver=1.7.21-wc.9.4.1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-includes/js/comment-reply.min.js?ver=6.7.1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-includes/js/dist/deprecated.min.js?ver=e1f84915c5e8ae38964c
Method	GET
Attack	
Evidence	
Other Info	

URL	https://hariyoilam.shop/wp-includes/js/dist/vendor/react-jsx-runtime.min.js?ver=18.3.1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-json/wc/store/v1/products/collection-data?min_price=&max_price=&calculate_price_range=true&_locale=user
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/wp-json/wc/store/v1?_locale=user
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/?wc-ajax=get_refreshed_fragments
Method	POST
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/?wc-ajax=update_order_review
Method	POST
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/?wc-ajax=wc_stripe_get_cart_details
Method	POST
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/?wc-ajax=wc_stripe_save_appearance
Method	POST
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/

Method	POST
Attack	
Evidence	
Other Info	
Instances	32
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://hariyoilam.shop/about/
Method	GET
Attack	
Evidence	1732237600
Other Info	1732237600, which evaluates to: 2024-11-21 19:06:40.
URL	https://hariyoilam.shop/about/
Method	GET
Attack	
Evidence	1732245123
Other Info	1732245123, which evaluates to: 2024-11-21 21:12:03.
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	1732237600
Other Info	1732237600, which evaluates to: 2024-11-21 19:06:40.
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	
Evidence	1732237600
Other Info	1732237600, which evaluates to: 2024-11-21 19:06:40.
URL	https://hariyoilam.shop/my-account/
Method	GET

Attack	
Evidence	1731600600
Other Info	1731600600, which evaluates to: 2024-11-14 10:10:00.
URL	https://hariyoilam.shop/my-account/
Method	GET
Attack	
Evidence	1732237600
Other Info	1732237600, which evaluates to: 2024-11-21 19:06:40.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	1732237600
Other Info	1732237600, which evaluates to: 2024-11-21 19:06:40.
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	1579042994
Other Info	1579042994, which evaluates to: 2020-01-14 17:03:14.
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	1732237600
Other Info	1732237600, which evaluates to: 2024-11-21 19:06:40.
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	1732909384
Other Info	1732909384, which evaluates to: 2024-11-29 13:43:04.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	1579042994
Other Info	1579042994, which evaluates to: 2020-01-14 17:03:14.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	1732237600

Other Info	1732237600, which evaluates to: 2024-11-21 19:06:40.
Instances	12
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	200
WASC Id	13
Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
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.
URL	https://hariyoilam.shop/about/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/my-account/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/

Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/elementor/assets/css/conditionals/dialog.min.css?ver=3.25.7
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/elementor/assets/css/conditionals/lightbox.min.css?ver=3.25.7
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/elementor/assets/js/lightbox.01a419d1fcdd47a75a77.bundle.min.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/elementor/assets/lib/dialog/dialog.min.js?ver=4.9.3
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client

	or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/elementor/assets/lib/jquery-numerator/jquery-numerator.min.js?ver=0.2.1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/elementor/assets/lib/share-link/share-link.min.js?ver=3.25.7
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/css/photoswipe/default-skin/default-skin.min.css?ver=9.4.1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/css/photoswipe/photoswipe.min.css?ver=9.4.1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/fonts/WooCommerce.woff
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/flexslider/jquery.flexslider.min.js?ver=2.7.2-wc.9.4.1
Method	GET
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/frontend/cart.min.js?ver=9.4.1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/frontend/single-product.min.js?ver=9.4.1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/photoswipe/photoswipe-ui-default.min.js?ver=4.1.1-wc.9.4.1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/photoswipe/photoswipe.min.js?ver=4.1.1-wc.9.4.1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/zoom/jquery.zoom.min.js?ver=1.7.21-wc.9.4.1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-includes/js/comment-reply.min.js?ver=6.7.1
Method	GET

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-includes/js/dist/deprecated.min.js?ver=e1f84915c5e8ae38964c
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/wp-includes/js/dist/vendor/react-jsx-runtime.min.js?ver=18.3.1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://r10.o.lencr.org/
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://r11.o.lencr.org/
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	27
	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.

Solution	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.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://hariyoilam.shop/about/
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 6 times, the first in the element starting with: "<script id="wc-add-to-cart-js-extra"> var wc_add_to_cart_params = {"ajax_url":"\/wp-admin\/admin-ajax.php","wc_ajax_url":"\/?wc-", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/about/
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> /(trident|msie)/i.test(navigator.userAgent)&&document.getElementById&&window.addEventListener&&window.addEventListen", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 12 times, the first in the element starting with: "<script id="wc-add-to-cart-js-extra"> var wc_add_to_cart_params = {"ajax_url":"\/wp-admin\/admin-ajax.php","wc_ajax_url":"\/?wc-", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	DB
Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "<script id="wc-country-select-js-extra"> var wc_country_select_params = {"countries":"{\"AF\":[],\"AL\":{\"AL-01\":\"Berat\",\"A", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	select

Other Info	The following pattern was used: \bSELECT\b and was detected 3 times, the first in the element starting with: "<script src="https://hariyoilam.shop/wp-content/plugins /woocommerce/assets/js/frontend/country-select.min.js?ver=9.4.1" id="wc-c", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 8 times, the first in the element starting with: "<script id="wc-add-to-cart-js-extra"> var wc_add_to_cart_params = {"ajax_url":"\/wp-admin\/admin-ajax.php","wc_ajax_url":"\/?wc-", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	
Evidence	DB
Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "<script id="wc-country-select-js-extra"> var wc_country_select_params = {"countries":"{\" AF\":[],\"AL\":{\"AL-01\":\"Berat\",\"A", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: "<script src="https://hariyoilam.shop/wp-content/plugins /woocommerce/assets/js/frontend/country-select.min.js?ver=9.4.1" id="wc-c", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/my-account/
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 10 times, the first in the element starting with: "<script id="wc-add-to-cart-js-extra"> var wc_add_to_cart_params = {"ajax_url":"\/wp-admin\/admin-ajax.php","wc_ajax_url":"\/?wc-", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/my-account/
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> /(trident|msie)/i.test(navigator.userAgent)&&document.getElementById&&window. addEventListener&&window.addEventListen", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	admin
Other	The following pattern was used: \bADMIN\b and was detected 10 times, the first in the element starting with: "<script id="wc-add-to-cart-js-extra"> var wc_add_to_cart_params =

Info	{"ajax_url":"\/wp-admin\/admin-ajax.php","wc_ajax_url":"\/?wc-", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	DB
Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "<script id="wc-country-select-js-extra"> var wc_country_select_params = {"countries":"{\"AF\":[],\"AL\":{\"AL-01\":\"Berat\",\"A", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "<script type="application/ld+json">{"@context":"https:\/\/schema.org\/","@type":"Product","@id":"https:\/\/hariyoilam.shop\/prod", see evidence field for the suspicious comment /snippet.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 4 times, the first in the element starting with: "<script id="wc-single-product-js-extra"> var wc_single_product_params = {"i18n_required_rating_text":"Please select a rating","r", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 10 times, the first in the element starting with: "<script id="wc-add-to-cart-js-extra"> var wc_add_to_cart_params = {"ajax_url":"\/wp-admin\/admin-ajax.php","wc_ajax_url":"\/?wc-", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: "<script id="wc-add-to-cart-variation-js-extra"> var wc_add_to_cart_variation_params = {"wc_ajax_url":"\/?wc-ajax=%%endpoint%%","", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/wp-content/plugins/elementor/assets/lib/dialog/dialog.min.js?ver=4.9.3
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "!function(t,e){"use strict";var n={widgetsTypes:{},createWidgetType:function(e,i,o){o||(o=this.Widget);var s=function(){o.apply(", see evidence field for the suspicious comment/snippet.

URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/frontend/cart.min.js?ver=9.4.1
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "jQuery(function(t){if("undefined"==typeof wc_cart_params)return!1;var e=function(t){return wc_cart_params.wc_ajax_url.toString()", see evidence field for the suspicious comment /snippet.
URL	https://hariyoilam.shop/wp-content/plugins/woocommerce/assets/js/frontend/single-product.min.js?ver=9.4.1
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "jQuery(function(t){if("undefined"==typeof wc_single_product_params)return!1;t("body").on ("init",".wc-tabs-wrapper, .woocommerce-", see evidence field for the suspicious comment /snippet.
URL	https://hariyoilam.shop/wp-includes/js/dist/deprecated.min.js?ver=e1f84915c5e8ae38964c
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "(()=>{"use strict";var e={d:(n,o)=>{for(var t in o)e.o(o,t)&&!e.o(n,t)&&Object.defineProperty (n,t,{enumerable:!0,get:o[t]})},o:(", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 10 times, the first in the element starting with: "<script id="wc-add-to-cart-js-extra"> var wc_add_to_cart_params = {"ajax_url":"\/wp-admin\/admin-ajax.php","wc_ajax_url":"\/?wc-", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	DB
Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "<script id="wc-country-select-js-extra"> var wc_country_select_params = {"countries":"{\"AF\":[],\"AL\":{\"AL-01\":\"Berat\",\"A", see evidence field for the suspicious comment/snippet.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "<script type="application/ld+json">{"@context":"https:\/\/schema.org\/","@type":"Product","@id":"https:\/\/hariyoilam.shop\/prod", see evidence field for the suspicious comment /snippet.

URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 4 times, the first in the element starting with: "<script id="wc-single-product-js-extra"> var wc_single_product_params = {"i18n_required_rating_text":"Please select a rating","r", see evidence field for the suspicious comment/snippet.
Instances	24
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200
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://hariyoilam.shop/about/
Method	GET
Attack	
Evidence	<a class="ast-header-account-link ast-account-action-link ast-header-account-type-icon" aria-label="Account icon link" href=/my-account target=_self > <span aria-hidden="true" class="ahfb-svg-iconset ast-inline-flex svg-baseline"><svg version='1.1' class='account-icon' xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x='0px' y='0px' viewBox='0 0 120 120' enable-background='new 0 0 120 120' xml:space='preserve'><path d='M84.6,62c-14.1,12.3-35.1,12.3-49.2,0C16.1,71.4,3.8,91,3.8,112.5c0,2.1,1.7,3.8,3.8,3.8h105c2.1,0,3.8-1.7,3.8-3.8 C116.2,91,103.9,71.4,84.6,62z'/><circle cx='60' cy='33.8' r='30'/></svg></span> </a>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
URL	https://hariyoilam.shop/cart/
Method	GET
Attack	
Evidence	<a class="ast-header-account-link ast-account-action-link ast-header-account-type-icon" aria-label="Account icon link" href=/my-account target=_self > <span aria-hidden="true" class="ahfb-svg-iconset ast-inline-flex svg-baseline"><svg version='1.1' class='account-icon' xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x='0px' y='0px' viewBox='0 0 120 120' enable-background='new 0 0 120 120' xml:space='preserve'><path d='M84.6,62c-14.1,12.3-35.1,12.3-49.2,0C16.1,71.4,3.8,91,3.8,112.5c0,2.1,1.7,3.8,3.8,3.8h105c2.1,0,3.8-1.7,3.8-3.8 C116.2,91,103.9,71.4,84.6,62z'/><circle cx='60' cy='33.8' r='30'/></svg></span> </a>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
URL	https://hariyoilam.shop/checkout/
Method	GET
Attack	
	<a class="ast-header-account-link ast-account-action-link ast-header-account-type-icon" aria-label="Account icon link" href=/my-account target=_self > <span aria-hidden="true" class="ahfb-svg-iconset ast-inline-flex svg-baseline"><svg version='1.1' class='account-icon' xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x='0px'

Evidence	y='0px' viewBox='0 0 120 120' enable-background='new 0 0 120 120' xml:space='preserve'><path d='M84.6,62c-14.1,12.3-35.1,12.3-49.2,0C16.1,71.4,3.8,91,3.8,112.5c0,2.1,1.7,3.8,3.8,3.8h105c2.1,0,3.8-1.7,3.8-3.8 C116.2,91,103.9,71.4,84.6,62z'/><circle cx='60' cy='33.8' r='30'/></svg></span> </a>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
URL	https://hariyoilam.shop/my-account/
Method	GET
Attack	
Evidence	<a class="ast-header-account-link ast-account-action-link ast-header-account-type-icon" aria-label="Account icon link" href=/my-account target=_self > <span aria-hidden="true" class="ahfb-svg-iconset ast-inline-flex svg-baseline"><svg version='1.1' class='account-icon' xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x='0px' y='0px' viewBox='0 0 120 120' enable-background='new 0 0 120 120' xml:space='preserve'><path d='M84.6,62c-14.1,12.3-35.1,12.3-49.2,0C16.1,71.4,3.8,91,3.8,112.5c0,2.1,1.7,3.8,3.8,3.8h105c2.1,0,3.8-1.7,3.8-3.8 C116.2,91,103.9,71.4,84.6,62z'/><circle cx='60' cy='33.8' r='30'/></svg></span> </a>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	<a class="ast-header-account-link ast-account-action-link ast-header-account-type-icon" aria-label="Account icon link" href=/my-account target=_self > <span aria-hidden="true" class="ahfb-svg-iconset ast-inline-flex svg-baseline"><svg version='1.1' class='account-icon' xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x='0px' y='0px' viewBox='0 0 120 120' enable-background='new 0 0 120 120' xml:space='preserve'><path d='M84.6,62c-14.1,12.3-35.1,12.3-49.2,0C16.1,71.4,3.8,91,3.8,112.5c0,2.1,1.7,3.8,3.8,3.8h105c2.1,0,3.8-1.7,3.8-3.8 C116.2,91,103.9,71.4,84.6,62z'/><circle cx='60' cy='33.8' r='30'/></svg></span> </a>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	<a class="ast-header-account-link ast-account-action-link ast-header-account-type-icon" aria-label="Account icon link" href=/my-account target=_self > <span aria-hidden="true" class="ahfb-svg-iconset ast-inline-flex svg-baseline"><svg version='1.1' class='account-icon' xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x='0px' y='0px' viewBox='0 0 120 120' enable-background='new 0 0 120 120' xml:space='preserve'><path d='M84.6,62c-14.1,12.3-35.1,12.3-49.2,0C16.1,71.4,3.8,91,3.8,112.5c0,2.1,1.7,3.8,3.8,3.8h105c2.1,0,3.8-1.7,3.8-3.8 C116.2,91,103.9,71.4,84.6,62z'/><circle cx='60' cy='33.8' r='30'/></svg></span> </a>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	<a class="ast-header-account-link ast-account-action-link ast-header-account-type-icon" aria-label="Account icon link" href=/my-account target=_self > <span aria-hidden="true" class="ahfb-svg-iconset ast-inline-flex svg-baseline"><svg version='1.1' class='account-icon' xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x='0px' y='0px' viewBox='0 0 120 120' enable-background='new 0 0 120 120' xml:

	space='preserve'><path d='M84.6,62c-14.1,12.3-35.1,12.3-49.2,0C16.1,71.4,3.8,91,3.8,112.5c0,2.1,1.7,3.8,3.8,3.8h105c2.1,0,3.8-1.7,3.8-3.8 C116.2,91,103.9,71.4,84.6,62z'/><circle cx='60' cy='33.8' r='30'/></svg></span> </a>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
Instances	7
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://hariyoilam.shop/about/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://hariyoilam.shop/shop/
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
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	Session Management Response Identified

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.
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	t_2ccf0378b3d0881bd363c1b3952abb%7C%7C1733249895%7C%7C1733246295%7C%7C4ec6680a72b08cff5659216c26f09720
Other Info	cookie:wp_woocommerce_session_b32934bef65fc6bdf351776efaf1c8dd cookie: woocommerce_cart_hash
URL	https://hariyoilam.shop/?wc-ajax=get_refreshed_fragments
Method	GET
Attack	
Evidence	8b3fe10092f6d176b555e83bdb4d4980
Other Info	json:cart_hash
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	GET
Attack	
Evidence	t_2ccf0378b3d0881bd363c1b3952abb%7C%7C1733249895%7C%7C1733246295%7C%7C4ec6680a72b08cff5659216c26f09720
Other Info	cookie:wp_woocommerce_session_b32934bef65fc6bdf351776efaf1c8dd
URL	https://hariyoilam.shop/?wc-ajax=get_refreshed_fragments
Method	POST
Attack	
Evidence	8b3fe10092f6d176b555e83bdb4d4980
Other Info	json:cart_hash
URL	https://hariyoilam.shop/product/wheat-from-organic-farms/
Method	POST
Attack	
Evidence	t_2ccf0378b3d0881bd363c1b3952abb%7C%7C1733249895%7C%7C1733246295%7C%7C4ec6680a72b08cff5659216c26f09720
Other Info	cookie:wp_woocommerce_session_b32934bef65fc6bdf351776efaf1c8dd
Instances	5
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112