

ZAP_{by} Checkmar× ZAP by Checkmarx Scanning Report

Site: https://beta.pupt-flss.com

Generated on Thu, 19 Dec 2024 17:39:06

ZAP Version: 2.15.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	2
Informational	3

Alerts

Name	Risk Level	Number of Instances
CSP: Wildcard Directive	Medium	4
CSP: script-src unsafe-inline	Medium	4
CSP: style-src unsafe-inline	Medium	4
Missing Anti-clickjacking Header	Medium	4
Strict-Transport-Security Header Not Set	Low	41
X-Content-Type-Options Header Missing	Low	41
Information Disclosure - Suspicious Comments	Informational	29
Modern Web Application	Informational	4
Re-examine Cache-control Directives	Informational	4

Alert Detail

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://beta.pupt-flss.com/
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://beta.pupt-flss.com/login
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://beta.pupt-flss.com/robots.txt
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://beta.pupt-flss.com/sitemap.xml
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.
Instances	4
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	<u>693</u>
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://beta.pupt-flss.com/
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://beta.pupt-flss.com/login
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://beta.pupt-flss.com/robots.txt
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://beta.pupt-flss.com/sitemap.xml
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
Instances	4
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	<u>693</u>
WASC Id	15
Plugin Id	<u>10055</u>
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://beta.pupt-flss.com/

Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://beta.pupt-flss.com/login
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://beta.pupt-flss.com/robots.txt
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://beta.pupt-flss.com/sitemap.xml
Method	GET
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
Instances	4
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	<u>10055</u>
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://beta.pupt-flss.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/login
Method	GET

Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	4
	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.
Solution	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	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://beta.pupt-flss.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/assets/images/pup_taguig_logo.svg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/assets/images/pupt_img_1.webp

Method	GET
Attack	
Evidence	
Other	
Info	
URL	https://beta.pupt-flss.com/assets/images/pupt_img_2.webp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/assets/images/pupt_img_3.webp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/assets/images/pupt_img_4.webp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/assets/images/pupt_img_5.webp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-3CIC7QKD.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-3LPJIGR4.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-42NUSC2L.js
Method	GET

E : 1	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-4SPUYEHS.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-4XL4JBVQ.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-5J32MMV4.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-7DAYRKTU.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-7UNGCTEQ.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-DBNUJAAA.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-EMZRNCIP.js
Method	GET
Attack	
Evidence	

Other	
Info	
URL	https://beta.pupt-flss.com/chunk-GFTFIPQ3.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-GZ4EGFK5.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-HB25W3BE.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-JJIJZYES.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-KA6B6XDT.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-O3XO7VNM.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-ODN5LVDJ.js
Method	GET
Attack	
Evidence	
Other Info	

URL	https://beta.pupt-flss.com/chunk-PPHBMCTZ.js
Method	GET
Attack	
Evidence	
Other	
Info	
URL	https://beta.pupt-flss.com/chunk-RWLBLQYG.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-SAURS5G2.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-SBV3OV3B.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-UXQSVLEZ.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-VGXYOY5L.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-W6BLF3IL.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-WYGBBPGQ.js
Method	GET

A 441-	
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-YAIF3KE2.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/chunk-Z2RZOCNL.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/login
Method	GET
Attack	
Evidence	
Other	
Info	
	https://beta.pupt-flss.com/main-2UGW37G2.js
Info	https://beta.pupt-flss.com/main-2UGW37G2.js GET
Info URL	
Info URL Method	
Info URL Method Attack	
Info URL Method Attack Evidence Other	
Info URL Method Attack Evidence Other Info	GET
Info URL Method Attack Evidence Other Info URL	https://beta.pupt-flss.com/media/Trajan-Pro-Semibold-XM5W3FX4.woff2
Info URL Method Attack Evidence Other Info URL Method	https://beta.pupt-flss.com/media/Trajan-Pro-Semibold-XM5W3FX4.woff2
Info URL Method Attack Evidence Other Info URL Method Attack	https://beta.pupt-flss.com/media/Trajan-Pro-Semibold-XM5W3FX4.woff2
Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other	https://beta.pupt-flss.com/media/Trajan-Pro-Semibold-XM5W3FX4.woff2
Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info	https://beta.pupt-flss.com/media/Trajan-Pro-Semibold-XM5W3FX4.woff2 GET
Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL URL Method Attack URL URL URL URL URL URL URL UR	https://beta.pupt-flss.com/media/Trajan-Pro-Semibold-XM5W3FX4.woff2 GET https://beta.pupt-flss.com/polyfills-FFHMD2TL.js
Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL Method Method Method Method	https://beta.pupt-flss.com/media/Trajan-Pro-Semibold-XM5W3FX4.woff2 GET https://beta.pupt-flss.com/polyfills-FFHMD2TL.js
Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack	https://beta.pupt-flss.com/media/Trajan-Pro-Semibold-XM5W3FX4.woff2 GET https://beta.pupt-flss.com/polyfills-FFHMD2TL.js
Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Other Info URL Method Attack Evidence Other Info	https://beta.pupt-flss.com/media/Trajan-Pro-Semibold-XM5W3FX4.woff2 GET https://beta.pupt-flss.com/polyfills-FFHMD2TL.js
Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Other Info URL Method Attack Evidence Other Info	https://beta.pupt-flss.com/media/Trajan-Pro-Semibold-XM5W3FX4.woff2 GET https://beta.pupt-flss.com/polyfills-FFHMD2TL.js GET
Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL URL URL URL URL URL	https://beta.pupt-flss.com/media/Trajan-Pro-Semibold-XM5W3FX4.woff2 GET https://beta.pupt-flss.com/polyfills-FFHMD2TL.js GET https://beta.pupt-flss.com/robots.txt

Evidence	
Other Info	
URL	https://beta.pupt-flss.com/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/styles-NS63FPTT.css
Method	GET
Attack	
Evidence	
Other Info	
Instances	41
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	<u>319</u>
WASC Id	15
WASC Id Plugin Id	15 10035
Plugin Id	10035
Plugin Id Low	X-Content-Type-Options Header Missing 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-
Plugin Id Low Description	X-Content-Type-Options Header Missing 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.
Plugin Id Low Description URL	X-Content-Type-Options Header Missing 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. https://beta.pupt-flss.com/
Plugin Id Low Description URL Method	X-Content-Type-Options Header Missing 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. https://beta.pupt-flss.com/
Plugin Id Low Description URL Method Attack	X-Content-Type-Options Header Missing 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. https://beta.pupt-flss.com/
Plugin Id Low Description URL Method Attack Evidence Other	X-Content-Type-Options Header Missing 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. https://beta.pupt-flss.com/ GET 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
Plugin Id Low Description URL Method Attack Evidence Other Info	X-Content-Type-Options Header Missing 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. https://beta.pupt-flss.com/ GET 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.
Plugin Id Low Description URL Method Attack Evidence Other Info URL	X-Content-Type-Options Header Missing 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. https://beta.pupt-flss.com/ GET 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. https://beta.pupt-flss.com/assets/images/pup_taguig_logo.svg
Plugin Id Low Description URL Method Attack Evidence Other Info URL Method	X-Content-Type-Options Header Missing 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. https://beta.pupt-flss.com/ GET 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. https://beta.pupt-flss.com/assets/images/pup_taguig_logo.svg
Plugin Id Low Description URL Method Attack Evidence Other Info URL Method Attack	X-Content-Type-Options Header Missing 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. https://beta.pupt-flss.com/ GET 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. https://beta.pupt-flss.com/assets/images/pup_taguig_logo.svg

	or server error responses.
URL	https://beta.pupt-flss.com/assets/images/pupt_img_1.webp
Method	GET
Attack	OE1
Evidence	
Evidence	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still
Other Info	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://beta.pupt-flss.com/assets/images/pupt_img_2.webp
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://beta.pupt-flss.com/assets/images/pupt_img_3.webp
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://beta.pupt-flss.com/assets/images/pupt_img_4.webp
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://beta.pupt-flss.com/assets/images/pupt_img_5.webp
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://beta.pupt-flss.com/chunk-3CIC7QKD.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://beta.pupt-flss.com/chunk-3LPJIGR4.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://beta.pupt-flss.com/chunk-42NUSC2L.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://beta.pupt-flss.com/chunk-4SPUYEHS.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://beta.pupt-flss.com/chunk-4XL4JBVQ.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://beta.pupt-flss.com/chunk-5J32MMV4.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://beta.pupt-flss.com/chunk-7DAYRKTU.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.

Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often affected by injection issues, in which case there is still concern for browsers sniffing page away from their actual content type. At "High" threshold this scan rule will not alert on clie or server error responses. URL https://beta.pupt-flss.com/chunk-DBNUJAAA.js Method GET Attack	es ent still
Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often affected by injection issues, in which case there is still concern for browsers sniffing page away from their actual content type. At "High" threshold this scan rule will not alert on clie or server error responses. URL https://beta.pupt-flss.com/chunk-DBNUJAAA.js Method GET Attack	es ent still
Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often affected by injection issues, in which case there is still concern for browsers sniffing page away from their actual content type. At "High" threshold this scan rule will not alert on clie or server error responses. URL https://beta.pupt-flss.com/chunk-DBNUJAAA.js Method GET Attack	es ent still
Other Info Other	es ent still
Other Info affected by injection issues, in which case there is still concern for browsers sniffing page away from their actual content type. At "High" threshold this scan rule will not alert on clie or server error responses. URL https://beta.pupt-flss.com/chunk-DBNUJAAA.js Method GET Attack	es ent still
Method GET Attack	
Attack	
Fridance	
Evidence	
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often affected by injection issues, in which case there is still concern for browsers sniffing page away from their actual content type. At "High" threshold this scan rule will not alert on clied or server error responses.	
URL https://beta.pupt-flss.com/chunk-EMZRNCIP.js	
Method GET	
Attack	
Evidence	
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often of affected by injection issues, in which case there is still concern for browsers sniffing page away from their actual content type. At "High" threshold this scan rule will not alert on clied or server error responses.	es
URL https://beta.pupt-flss.com/chunk-GFTFIPQ3.js	
Method GET	
Attack	
Evidence	
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often affected by injection issues, in which case there is still concern for browsers sniffing page away from their actual content type. At "High" threshold this scan rule will not alert on clied or server error responses.	es
URL https://beta.pupt-flss.com/chunk-GZ4EGFK5.js	
Method GET	
Attack	
Evidence	
Other Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often affected by injection issues, in which case there is still concern for browsers sniffing page away from their actual content type. At "High" threshold this scan rule will not alert on clied or server error responses.	es
URL https://beta.pupt-flss.com/chunk-HB25W3BE.js	
Method GET	
Attack	
Evidence	
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often Other affected by injection issues, in which case there is still concern for browsers sniffing page away from their actual content type. At "High" threshold this scan rule will not alert on clied or server error responses.	es
URL https://beta.pupt-flss.com/chunk-JJIJZYES.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://beta.pupt-flss.com/chunk-KA6B6XDT.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://beta.pupt-flss.com/chunk-O3XO7VNM.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://beta.pupt-flss.com/chunk-ODN5LVDJ.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://beta.pupt-flss.com/chunk-PPHBMCTZ.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://beta.pupt-flss.com/chunk-RWLBLQYG.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://beta.pupt-flss.com/chunk-SAURS5G2.js

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. https://beta.pupt-flss.com/chunk-SBV3OV3B.js GET 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. https://beta.pupt-flss.com/chunk-UXQSVLEZ.js GET 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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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
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. https://beta.pupt-flss.com/chunk-SBV3OV3B.js GET 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. https://beta.pupt-flss.com/chunk-UXQSVLEZ.js GET 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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages
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. https://beta.pupt-flss.com/chunk-SBV3OV3B.js GET 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. https://beta.pupt-flss.com/chunk-UXQSVLEZ.js GET 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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages
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. https://beta.pupt-flss.com/chunk-SBV3OV3B.js GET 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. https://beta.pupt-flss.com/chunk-UXQSVLEZ.js GET 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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages
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. https://beta.pupt-flss.com/chunk-UXQSVLEZ.js GET 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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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
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. https://beta.pupt-flss.com/chunk-UXQSVLEZ.js GET 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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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
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. https://beta.pupt-flss.com/chunk-UXQSVLEZ.js GET 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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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
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. https://beta.pupt-flss.com/chunk-UXQSVLEZ.js GET 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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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
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. https://beta.pupt-flss.com/chunk-UXQSVLEZ.js GET 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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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
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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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
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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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
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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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
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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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
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. https://beta.pupt-flss.com/chunk-VGXYOY5L.js GET 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
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
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
affected by injection issues, in which case there is still concern for browsers sniffing pages
affected by injection issues, in which case there is still concern for browsers sniffing pages
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.
https://beta.pupt-flss.com/chunk-W6BLF3IL.js
GET
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.
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
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.
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. https://beta.pupt-flss.com/chunk-WYGBBPGQ.js
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. https://beta.pupt-flss.com/chunk-WYGBBPGQ.js
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. https://beta.pupt-flss.com/chunk-WYGBBPGQ.js
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. https://beta.pupt-flss.com/chunk-WYGBBPGQ.js GET 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. https://beta.pupt-flss.com/chunk-W6BLF3IL.js

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://beta.pupt-flss.com/chunk-Z2RZOCNL.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://beta.pupt-flss.com/login
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://beta.pupt-flss.com/main-2UGW37G2.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://beta.pupt-flss.com/media/Trajan-Pro-Semibold-XM5W3FX4.woff2
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://beta.pupt-flss.com/polyfills-FFHMD2TL.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://beta.pupt-flss.com/robots.txt
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://beta.pupt-flss.com/sitemap.xml
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://beta.pupt-flss.com/styles-NS63FPTT.css
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.
Instances	41
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
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

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://beta.pupt-flss.com/chunk-3CIC7QKD.js
Method	GET
Attack	
Evidence	Query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "var i=function(e){return e[e.State=0]="State",e[e.Transition=1]="Transition",e[e. Sequence=2]="Sequence",e[e.Group=3]="Group",e[e", see evidence field for the suspicious comment/snippet.
URL	https://beta.pupt-flss.com/chunk-3LPJIGR4.js
Method	GET
Attack	

Friday	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "import{c as n,d as a,g as t,h as r,j as e,l as i,m as o}from"./chunk-3CIC7QKD.js";var c=n ("fadeAnimation",[e("* <=> *",[t({opaci", see evidence field for the suspicious comment /snippet.
URL	https://beta.pupt-flss.com/chunk-42NUSC2L.js
Method	GET
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "`)}`} var II=vl(ul("Optional"),8);var EI=vl(ul("SkipSelf"),4);function it(e,t){let n=e.hasOwnProperty (Mr);return n?e[Mr]:null}f", see evidence field for the suspicious comment/snippet.
URL	https://beta.pupt-flss.com/chunk-42NUSC2L.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "import{a as ee,b as te}from"./chunk-ODN5LVDJ.js";function m(e){return typeof e=="function"}function bt(e){let n=e(r=>{Error.call", see evidence field for the suspicious comment /snippet.
URL	https://beta.pupt-flss.com/chunk-42NUSC2L.js
Method	GET
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected in the element starting with: "`)}`:"",this.name="UnsubscriptionError",this.errors=n});function Ge(e,t){if(e){let n=e.indexOf (t);0<=n&e.splice(n,1)}}var L=c", see evidence field for the suspicious comment/snippet.
URL	https://beta.pupt-flss.com/chunk-4SPUYEHS.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "import{a as Y}from"./chunk-O3XO7VNM.js";import{a as b}from"./chunk-YAIF3KE2.js";import {d as R}from"./chunk-RWLBLQYG.js";import{a", see evidence field for the suspicious comment/snippet.
URL	https://beta.pupt-flss.com/chunk-4XL4JBVQ.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "import{a as ht,c as ut}from"./chunk-W6BLF3IL.js";import{a as lt,e as dt,h as mt}from". /chunk-GZ4EGFK5.js";import{m as l,n as ot,", see evidence field for the suspicious comment /snippet.
URL	https://beta.pupt-flss.com/chunk-5J32MMV4.js
Method	GET
Attack	
Evidence	query
	The following pattern was used: \bQUERY\b and was detected in the element starting with:

Other Info	"import{d as y,w as Mt}from"./chunk-KA6B6XDT.js";import{\$ as p,Aa as I,Ab as te,Ba as Ee, Bc as Et,Cb as z,Cc as At,D as S,Da as A", see evidence field for the suspicious comment /snippet.
URL	https://beta.pupt-flss.com/chunk-7DAYRKTU.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "import{\$a as n,Aa as a,jb as s,la as i}from"./chunk-42NUSC2L.js";var o=(()=>{class e{el; name="";variant="rounded";fill=!0;weight", see evidence field for the suspicious comment /snippet.
URL	https://beta.pupt-flss.com/chunk-7UNGCTEQ.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "import{a as E,b as B,f as mt,g as Ne,n as x,o as Me,p as ue}from"./chunk-3CIC7QKD.js"; import"./chunk-KA6B6XDT.js";import{X as S,", see evidence field for the suspicious comment/snippet.
URL	https://beta.pupt-flss.com/chunk-DBNUJAAA.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "import{d as le,k as de,z as he}from"./chunk-KA6B6XDT.js";import{C as H,Fa as ce,J as ee, T as ne,X as re,_ as O,ba as N,c as X,da", see evidence field for the suspicious comment /snippet.
URL	https://beta.pupt-flss.com/chunk-DBNUJAAA.js
Method	GET
Attack	
Evidence	User
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "`). for Each(n=>{let t=n.indexOf(":");if(t>0){let s=n.slice(0,t),i=n.slice(t+1).trim();this. addHeaderEntry(s,i)}})}:typeof Headers", see evidence field for the suspicious comment /snippet.
URL	https://beta.pupt-flss.com/chunk-GFTFIPQ3.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "import{a as P,b as re,c as oe,d as f,k as se,v as ie,x as H,z as ae}from"./chunk-KA6B6XDT. js";import{Ca as G,Da as N,Ea as Y,Fa ", see evidence field for the suspicious comment /snippet.
URL	https://beta.pupt-flss.com/chunk-GZ4EGFK5.js
Method	GET
Attack	
Evidence	from
Other	The following pattern was used: \bFROM\b and was detected in the element starting with: "import{h as H,j as D,l as V,n as kt,p as Ot,s as St}from"./chunk-Z2RZOCNL.js";import{L as

Info	bt,M as F,N as wt,a as R,e as vt,h as ", see evidence field for the suspicious comment /snippet.
URL	https://beta.pupt-flss.com/chunk-HB25W3BE.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "import{d as I,w as h}from"./chunk-KA6B6XDT.js";import{Fa as m,_ as p,da as f}from". /chunk-42NUSC2L.js";var R=(()=>{class i{const", see evidence field for the suspicious comment/snippet.
URL	https://beta.pupt-flss.com/chunk-JJIJZYES.js
Method	GET
Attack	
Evidence	Db
Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "import{O as I}from"./chunk-5J32MMV4.js";import{r as W}from"./chunk-KA6B6XDT.js";import {\$ as h,Aa as y,Ab as d,Bb as I,Cb as C,Db", see evidence field for the suspicious comment /snippet.
URL	https://beta.pupt-flss.com/chunk-KA6B6XDT.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "import{\$ as Ee,\$a as g,Aa as N,Bc as ve,Cc as J,Dc as le,Ec as Me,Fa as we,Jc as Q,Tb as m,Ub as f,X as Ce,Y as Fe,Za as Ae,_ as", see evidence field for the suspicious comment/snippet.
URL	https://beta.pupt-flss.com/chunk-O3XO7VNM.js
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "import{d as i}from"./chunk-RWLBLQYG.js";import{_ as o,da as a}from"./chunk-42NUSC2L. js";var m=(()=>{class e{router;roleHomeMap={", see evidence field for the suspicious comment/snippet.
URL	https://beta.pupt-flss.com/chunk-PPHBMCTZ.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "import{a as h}from"./chunk-O3XO7VNM.js";import{a as l}from"./chunk-YAIF3KE2.js";import {d as a}from"./chunk-RWLBLQYG.js";import{a", see evidence field for the suspicious comment/snippet.
URL	https://beta.pupt-flss.com/chunk-RWLBLQYG.js
Method	GET
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "import{c as Jr}from"./chunk-GFTFIPQ3.js";import{d as Qr,e as Kr,f as Se,g as Zr,h as Yr,i as Re,y as Xr}from"./chunk-KA6B6XDT.js", see evidence field for the suspicious comment

Info ZRZOCNL;s';mport(] as \$,K as Q,M as ", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-filss.com/chunk-SBY3OV3B.js Method GET Attack Evidence The following pattern was used: 'bFROMb and was detected in the element starting with: 'import(] as De,b as Ae,c as Q,e as p,h as Pjfrom' /chunk-GZ4EGFK5,js';mport(] as ve,m as Y,n as be,o as Ce,r as b,s as C;from'.', see evidence field for the suspicious comment /snippet. URL https://beta.pupt-filss.com/chunk-UXQSVLEZ.js Method GET Attack Evidence from The following pattern was used: 'bFROMb and was detected in the element starting with: "import(] as oe)from'./chunk-RAGBSXDT.js';import(] as U,Sa as o.Aa as ne,Cb as re,Cc as be,Gc as se,Ic as M,Jc as p,Vb as N,X as ", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-filss.com/chunk-VGXYOY5L.js Method GET Attack Evidence Db The following pattern was used: 'bDBbb and was detected in the element starting with: 'import(] as vylfrom'./chunk-DSNUJAAA.js':import(] as Y)from'./chunk-GFTFIPQ3.js'; import(] as Vylfrom'./chunk-DSNUJAAA.js':import(] as Y)from'./chunk-GFTFIPQ3.js'; import(] as Sylfrom'./chunk-DSNUJAAA.js':import(] as Cylfrom'./chunk-GFTFIPQ3.js'; import(] as Sylfrom'.ys p,Jchunk-WGBLF3IL.js Method GET Attack Evidence Db The following pattern was used: 'bDBbb and was detected in the element starting with: 'import(] as Sylfrom'.ys p,Jchunk-WGBLF3IL.js GET Attack Evidence Db The following pattern was used: 'bDBbb and was detected in the element starting with: 'import(] as a, h,Cb as d,Db as b,Ga as x,Gc a', see evidence field for the suspicious comment /snippet. URL https://beta.pupt-filss.com/chunk-WYGBBPGQ.js The following pattern was used: 'bFROMb and was detected in the element starting with: 'import(] as s,g, as a)from'.ychunk-42NUSC2L.js',var me([)—>(class e)filsofarTheme=new e info 'lisibarThemes as observar', see evidence field for the suspicious comment 'lisibarThemes as observar', see evidence field for the sus		/snippet.
Evidence The following pattern was used: 'bFROMb and was detected in the element starting with: 'mpont(e as c.h as tt)from'./chunk-GZ4EGFK5.js*;import(fh as q.k as K.m as J)from'./chunk ZRZCOCNL.js*;import(l as \$,K as Q.M as *, see evidence field for the suspicious comment /snippet. URL https://beta.pupl-filss.com/chunk-SBV3OV3B.js Method GET Attack Evidence The following pattern was used: 'bFROMb and was detected in the element starting with: 'mpont(a as De.b as Ae.c as Q.e as p.h as P)from'./chunk-GZ4EGFK5.js*;impont(i as ve.m as *, na as be, oa s C.e, ra s b.s as C)from'.*, see evidence field for the suspicious comment /snippet. URL Method GET Attack Evidence from The following pattern was used: 'bFROMb and was detected in the element starting with: "mpont(a as oe)from'./chunk-GABGXDT.js*;impont(i as as o., Aa as ne, Cb as re, Cc as the Cas as e.g. as m.y.b as N.X as *, see evidence field for the suspicious comment /snippet. URL https://beta.pupl-filss.com/chunk-USQXYOY5L.js Method GET Attack Evidence Db The following pattern was used: 'bDBbb and was detected in the element starting with: 'mpont(O as wifrom'./chunk-DBNUJAAA.js*;impont(d' as Y)from'./chunk-GFTEIPQ3.js*; import(c as V)from'./chunk-DBNUJAAA.js*;import(d' as Y)from'./chunk-GFTEIPQ3.js*; import(c as V)from'./chunk-DBNUJAAA.js*;import(d'); see evidence field for the suspicious comment /snippet. URL Method GET Attack Evidence Db The following pattern was used: 'bDBbb and was detected in the element starting with: 'mpont(O as W)from'./chunk-DBNUJAAA.js*;import(d'); see evidence field for the suspicious comment /snippet. URL https://beta.pupl-filss.com/chunk-WYGBPGQ.js Method GET Attack Evidence The following pattern was used: 'bDROMb and was detected in the element starting with: 'mpont(a as B,l,O as p,X as F,a as z,J as A,Ja as C)from'./chunk-SJ32MMV4.js*;import(s as f,as as B,Cb as G,Db as b,Ga as x,Gc a*, see evidence field for the suspicious comment /snippet.	URL	https://beta.pupt-flss.com/chunk-SAURS5G2.js
Evidence from The following pattern was used: 'bFROM'b and was detected in the element starting with: "Import(e as c.h as tt)/from'./chunk-GZ4EGFK5 js";import(h as q.k as K,m as J)/from'./chunk-GZ4EGFK5 js";import(h as q.k as K,m as J)/from'./chunk-GZ4EGFK5 js";import(h as q.k as K,m as J)/from'./chunk-GXIBQFK6 URL https://beta.pupt-filss.com/chunk-SBY3OV3B.js Method GET	Method	GET
The following pattern was used: 'bFROMb and was detected in the element starting with: 'import(e as c, h as til)from'./chunk-G24EGFK5,is'.import(h as q,k as K,m as J)from'./chunk 2/R2CORLI,s'.import(l as \$,k as Q,M as ", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-fiss.com/chunk-SBV3OV3B.js Method GET Attack Evidence from The following pattern was used: 'bFROMb and was detected in the element starting with:	Attack	
Other Info ZRZCONL, is "import(a as £,h as til)from" /chunk-CZ4EGFK5,is "import(h as &,k as K,m as J)from" /chunk-Snippet. URL https://beta.pupt-filss.com/chunk-SBV3OV3B.js Method GET Attack Evidence from The following pattern was used: 'bFROM'b and was detected in the element starting with: "import(a as De,b as Ae, as Q,e as p,h as P)from" /chunk-GZ4EGFK5,is "import(ia as vern as Y,n as be,o as Ce,r as b,s as C)from".' see evidence field for the suspicious comment /snippet. URL https://beta.pupt-filss.com/chunk-UXQSVLEZ.js Method GET Attack Evidence from The following pattern was used: 'bFROM'b and was detected in the element starting with: "import(a as vern as be, as as C), as b, as C), as b, as as 0, as as e, cb as c, ca s, ch as b, as c, ca s, ca as b, as as c, ca as b, ca as c, ca as comment comment starting with: Other import(as s) Virtom 'chunk-WGBBPQQ.js The following pattern was used: 'bDRbb and was detected in the element starting with: Other import(as as c, ca as collected in the element starting with: Other import(ca s) Virtom 'chunk-WGBBPQQ.js	Evidence	from
Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: \text{"import(a as De,b as Ae,c as Q,e as p,h as P}\text{"from".'\chunk-GZ4EGFK5,is";\text{"import(i as ve,m as Y,n as be,o as Ce,r as b,s as C}\text{"from".'\chunk-GZ4EGFK5,is";\text{"import(i as ve,m as Y,n as be,o as Ce,r as b,s as C}\text{"from".'\chunk-GZ4EGFK5,is";\text{"import(i as ve,m as Y,n as be,o as Ce,r as b,s as C}\text{"from".'\chunk-GSVLEZ.\text{"js}} Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: \text{"import(a as oe)\text{"from".'\chunk-KA6B6XDT.\js";\text{"import(\$ as u,\$ as a o, Aa as ne,C b as re,C c a be,G c as se,Ic as M,Jc as p,V b as N,X as", see evidence field for the suspicious comment \text{\sinport(b as ve,C c as se,Ic as M,Jc as p,V b as N,X as", see evidence field for the suspicious comment \text{\sinport(b as ve,C c as se,Ic as M,Jc as p,V b as N,X as", see evidence field for the suspicious comment \text{\sinport(b as ve,C c as se,Ic as se,Ic as as evidence \text{"from".\chunk-DBNUJAAA.\js";\text{"import(a as Y\from".\chunk-GFTFIPQ3.\js";\text{"import(a as Y\from".\chunk-GFTFIPQ3.\js";\text{"import(a as Y\from".\chunk-GFTFIPQ3.\js";\text{"import(a as Y\from".\chunk-GFTFIPQ3.\js";\text{"import(a as Y\from".\chunk-GFTFIPQ3.\js";\text{"import(a as A, b,C as a, b,C as a, b,C as as z,J as as z,J as A,J as as C\from".\chunk-SJ32MMV4,\js";\text{"import(\$ as t,J as a,L as a,L as as z,J as as z,J as as C\from".\chunk-SJ32MMV4,\js";\text{"import(\$ as a,L b,C as a,L b,C as a,L b,C as z,L		"import{e as c,h as tt}from"./chunk-GZ4EGFK5.js";import{h as q,k as K,m as J}from"./chunk-Z2RZOCNL.js";import{I as \$,K as Q,M as ", see evidence field for the suspicious comment
Attack Evidence The following pattern was used: 'bFROM'b and was detected in the element starting with: "import(a as De,b as Ae,c as Q.e as p.h as P)from"./chunk-GZ4EGFK5,js";import(j as ve,m as Ve,n as be,o as Ce,r as b,s as C)from".", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-UXQSVLEZ.js Method GET The following pattern was used: 'bFROM'b and was detected in the element starting with: "import(a as oe)from"./chunk-KAB6K0T.js";import(§ as U.\$a as o.Aa as ne,Cb as re, Cc as be,Gc as se,Ic as M,Jc as p,Vb as N,X as ", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-VGXYOY5L.js Method GET Attack Evidence Db The following pattern was used: 'bDB'b and was detected in the element starting with: "import() as w)from"./chunk-SJ32MMV4.js";import(d as Y)from"./chunk-GFTFIPQ3.js"; import() as w)from"./chunk-DBNUJAAA.js";import(d", see evidence field for the suspicious comment/snippet. URL https://beta.pupt-flss.com/chunk-W6BLF3IL.js Method GET Attack Evidence Db The following pattern was used: 'bDB'b and was detected in the element starting with: "import() as V)from"./chunk-DBNUJAAA.js";import(d", see evidence field for the suspicious comment/snippet. URL https://beta.pupt-flss.com/chunk-W6BLF3IL.js Method GET Attack Evidence Db The following pattern was used: 'bDB'b and was detected in the element starting with: "import() as B,I,O as p,X as F,a as z,j as A,ja as C)from"./chunk-SJ32MMV4.js";import(§ as f,Aa as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment // snippet. Ittps://beta.pupt-flss.com/chunk-WYGBBPGQ.js Method GET The following pattern was used: 'bFROM'b and was detected in the element starting with: "import(_ as s,g as a)from"./chunk-42NUSC2L.js";var m=(()=>(class e(sDarkTheme==new a)from"./chunk-642NUSC2L.js";var m=(()=>(class e(sDarkTheme==new a)from"./chunk-642NUSC2L.js",var m=(()=>(class e(sDarkTheme==new a)from //chunk-642NUSC2L.js",var m=((URL	https://beta.pupt-flss.com/chunk-SBV3OV3B.js
The following pattern was used: 'bFROM'b and was detected in the element starting with: "import(a as De,b as Ae,c as Q,e as p.h as P]from"/chunk-GZ4EGFK5,is*:import(i as ve,m as Ve,o as Ce,r as b,s as C)from".", see evidence field for the suspicious comment /snippet. URL Method GET Attack Evidence The following pattern was used: 'bFROM'b and was detected in the element starting with: "import(a as oe)from"/chunk-KA6B6XDT.js*:import(\$ as U,\$a as o.Aa as ne,Cb as re,Cc as be,Gc as se,Ic as M,Jc as p,Vb as N,X as ", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-fiss.com/chunk-VGXYOY5L.js Method GET Attack Evidence Db The following pattern was used: 'bDB\b and was detected in the element starting with: "import(a as v)from"/chunk-GYXYOY5L.js Method GET Attack Evidence Db The following pattern was used: 'bDB\b and was detected in the element starting with: "import(O as w)from"/chunk-D3DNUJAAA.js*:import(d as Y)from"/chunk-GFTFIPQ3.js*; import(C as V)from*/chunk-DBNUJAAA.js*:import(d*, see evidence field for the suspicious comment/snippet. URL https://beta.pupt-fiss.com/chunk-W6BLF3IL.js Method GET Attack Evidence Db The following pattern was used: 'bDB\b and was detected in the element starting with: "import(S as B,I,O as p,X as F,a as z,I as A,Ia as C)from"/chunk-5J32MMV4,is*:import(\$ as C) as as a comment /snippet. URL https://beta.pupt-fiss.com/chunk-WYGBBPGQ.js Method GET Attack Evidence from The following pattern was used: 'bFROM'b and was detected in the element starting with: "import(C as S,g as a)from"/chunk-4JUSC2L.js*; var m=((D=>classe ejsbarkTheme=new einter) = fischarkTheme=new einterser*, see evidence field for the suspicious comment /snippet. Other import(C as S,g as a)from*/chunk-4VUSC2L.js*; var m=((D=>classe ejsbarkTheme=new einterser*) = fischarkTheme=new einterser*, see evidence field for the suspicious	Method	GET
The following pattern was used: 'bFROM'b and was detected in the element starting with: "import(a as De,b as Ae,c as Q,e as p,h as P)from"/chunk-GZ4EGFK5,is":import(i as ve.m as Y,n as be,o as Ce,r as b,s as C)from".", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-UXQSVLEZ.js Method GET Attack Evidence from The following pattern was used: 'bFROM'b and was detected in the element starting with: "import(a as oe)from"./chunk-KA6B6XDT.js":import(\$ as U,\$a as o,Aa as ne,Cb as re,Cc as be,Gc as se,Ic as M,Jc as p,Vb as N,X as ", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-VGXYOY5L.js Method GET Attack Evidence Db The following pattern was used: 'bDB\b and was detected in the element starting with: "import(a as Y)from"./chunk-DBNUJAAA.js":import(d as Y)from"./chunk-GFTFIPQ3.js"; import(a as Y)from"./chunk-DBNUJAAA.js":import(d", see evidence field for the suspicious comment/snippet. URL https://beta.pupt-flss.com/chunk-W6BLE3IL.js Method GET Attack Evidence Db The following pattern was used: 'bDB\b and was detected in the element starting with: "import(a sa y)from"./chunk-GJ32MMV4.js";import(d", see evidence field for the suspicious comment/snippet. URL https://beta.pupt-flss.com/chunk-W6BLE3IL.js GET Attack Evidence Db The following pattern was used: 'bDB\b and was detected in the element starting with: "import(s as B,I,O as p,X as F,a as z,J as A,Ja as C)from"./chunk-6J32MMV4.js";import(\$ as Y)from some field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-WYGBBPGQ.js Method GET Attack Evidence from The following pattern was used: 'bFROM'b and was detected in the element starting with: "import(_ as s,g as a)from"./chunk-4ZNUSC2L.js",var m=((p=-classe ejisDarkTheme-enew einemenew	Attack	
Other Info as P., as be, o as Ce, r as b, s as P.) from"./-chunk-GZ4EGFK5, js";import(i as ve, m as Y, n as be, o as Ce, r as b, s as C) from".", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-fiss.com/chunk-UXQSVLEZ.js Method GET Attack Evidence from The following pattern was used: 'bFROMb and was detected in the element starting with: "import(a as oe) from"./chunk-KA6B6XDT, js";import(§ as U, Sa as o, Aa as ne, Cb as re, Cc as be, Gc as se, lc as M, Jc as p, Vb as N, X as ", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-fiss.com/chunk-VGXYOY5L.js Method GET Attack Evidence Db The following pattern was used: 'bDB\b and was detected in the element starting with: "import(as y) from"./chunk-5J32MMV4, js":import(d as Y) from"./chunk-GFTFIPQ3, js"; import(d as Y)	Evidence	from
Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: "import(a as oe)from"./chunk-KA6B6XDT.js";import(\\$ as U.\\$ as a, \A as ne, Cb as re, Cc at be, Gc as se, Ic as M.\Jc as p.\Vb as N,X as ", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-VGXYOY5L.js Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import(\cas \wightarrow\)"rom"./chunk-\s\J32MMV4.js";import(\cas \wightarrow\)"rom"./chunk-\GFTFIPQ\J3.js"; import(\cas \wightarrow\)"rom\)"/chunk-DBNUJAAA,js";import(\cas \wightarrow\)", see evidence field for the suspicious comment/snippet. URL https://beta.pupt-flss.com/chunk-W6BLF3IL.js Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import(\sa \wightarrow\)" as \wightarrow\) as \wightarrow as \wightarrow as \wightarrow\); as \wightarrow as \wightarrow\); as \wightarrow as \w		"import{a as De,b as Ae,c as Q,e as p,h as P}from"./chunk-GZ4EGFK5.js";import{i as ve,m as Y,n as be,o as Ce,r as b,s as C}from".", see evidence field for the suspicious comment
Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: "import(a as oe)from"./chunk-KA6B6XDT.js";import(\$ as U,\$a as o,Aa as ne,Cb as re,Cc as be,Gc as se,Ic as M,Jc as p,Vb as N,X as ", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-VGXYOY5L.js Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import(O as w)from"./chunk-5J32MMV4.js";import(d as Y)from"./chunk-GFTFIPQ3.js"; infor import(c as V)from"./chunk-DBNUJAAA.js";import(d", see evidence field for the suspicious comment/snippet. URL https://beta.pupt-flss.com/chunk-W6BLF3IL.js Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import(s as B,I,O as p,X as F,a as z,j as A,ja as C)from"./chunk-5J32MMV4.js";import(\$ as f,Aa as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-WYGBBPGO.js Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: "import(_as s,g as a)from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new are import(_as s,g as a)from"./chunk-42NUSC2L.js";var m=()=>{class e{isDark	URL	https://beta.pupt-flss.com/chunk-UXQSVLEZ.js
Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: "import{a as oe}from"./chunk-KA6B6XDT.js";import{\$ as U,\$a as o,Aa as ne,Cb as re,Cc as be,Gc as se,Ic as M,Jc as p,Vb as N,X as ", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-VGXYOY5L.js Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import{O as w}from"./chunk-5J32MMV4.js";import{d as Y}from"./chunk-GFTFIPQ3.js"; import{C as V}from"./chunk-DBNUJAAA.js";import{d", see evidence field for the suspicious comment/snippet. URL https://beta.pupt-flss.com/chunk-W6BLF3IL.js Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import{S as B,I,O as p,X as F,a as z,j as A,ja as C}from"./chunk-5J32MMV4.js";import{\$ as C}from"./chunk-5J32MMV4.js";import{} as C}from"./chunk-5J32MMV4.js";import{\$ as C}from"./chunk-5J32MMV4.js";import{\$ as C}from"./chunk-5J32MMV4.js";import{\$ as C}from"./chunk-5J32MMV4.js";import{\$ as C}from"./chunk-5J32MMV4.js";import{\$ as C}from"./chunk-5J32MMV4.js";import{\$ as C}from"./chu	Method	GET
The following pattern was used: \bFROM\b and was detected in the element starting with: "import{a as oe}from"./chunk-KA6B6XDT.js";import{\$ as U,\$a as o,Aa as ne,Cb as re,Cc as be,Gc as se,Ic as M,Jc as p,Vb as N,X as ", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-fiss.com/chunk-VGXYOY5L.js Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import{0 as w}from"./chunk-5J32MMV4.js";import{d as Y}from"./chunk-GFTFIPQ3.js"; import{c as V}from"./chunk-DBNUJAAA.js";import{d", see evidence field for the suspicious comment/snippet. URL https://beta.pupt-fiss.com/chunk-W6BLF3IL.js Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import{\$ as B,I,O as p,X as F,a as z,j as A,ja as C}from"./chunk-5J32MMV4.js";import{\$ as Info f,Aa as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-fiss.com/chunk-WYGBBPGQ.js Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a Info following pattern was used: \bFROM\b and was detected in the element starting with: "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a Info following pattern was used: \bFROM\b and was detected in the element starting with: "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a Info following pattern was used: \bFROM\b and was detected in the element starting with: "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a Info following pattern was used: \bFROM\b and was detected in the element starting with:	Attack	
Other Info	Evidence	from
Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import(O as w)from"./chunk-5J32MMV4.js",import{d as Y}from"./chunk-GFTFIPQ3.js"; Info import(c as V)from"./chunk-DBNUJAAA.js",import{d", see evidence field for the suspicious comment/snippet. URL https://beta.pupt-flss.com/chunk-W6BLF3IL.js Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import{s as B,I,O as p,X as F,a as z,j as A,ja as C}from"./chunk-5J32MMV4.js";import{\$ as f,Aa as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-WYGBBPGQ.js Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a 1}isbarkTheme}=new a 1);isDarkTheme\$=this.isDarkTheme.asObserva", see evidence field for the suspicious		"import{a as oe}from"./chunk-KA6B6XDT.js";import{\$ as U,\$a as o,Aa as ne,Cb as re,Cc as be,Gc as se,Ic as M,Jc as p,Vb as N,X as ", see evidence field for the suspicious comment
Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import(O as w)from"./chunk-5J32MMV4.js";import(d as Y)from"./chunk-GFTFIPQ3.js"; Info import(c as V)from"./chunk-DBNUJAAA.js";import(d", see evidence field for the suspicious comment/snippet. URL https://beta.pupt-flss.com/chunk-W6BLF3IL.js Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import(\$ as B,I,O as p,X as F,a as z,j as A,ja as C)from"./chunk-5J32MMV4.js";import(\$ as f,Aa as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-WYGBBPGQ.js Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: "import(_ as s,g as a)from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a logical parkTheme} = logical parkTheme = logical parkThe	URL	https://beta.pupt-flss.com/chunk-VGXYOY5L.js
Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import{O as w}from"./chunk-5J32MMV4.js";import{d as Y}from"./chunk-GFTFIPQ3.js"; import{c as V}from"./chunk-DBNUJAAA.js";import{d", see evidence field for the suspicious comment/snippet. URL https://beta.pupt-flss.com/chunk-W6BLF3IL.js Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import{\$ as B,I,O as p,X as F,a as z,j as A,ja as C}from"./chunk-5J32MMV4.js";import{\$ as I,Aa as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-WYGBBPGQ.js Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e}(isDarkTheme=new a I);isDarkTheme\$=this.isDarkTheme.asObserva", see evidence field for the suspicious	Method	GET
The following pattern was used: \bDB\b and was detected in the element starting with: "import{O as w}from"./chunk-5.J32MMV4.js";import{d as Y}from"./chunk-GFTFIPQ3.js"; import{c as V}from"./chunk-DBNUJAAA.js";import{d", see evidence field for the suspicious comment/snippet. URL https://beta.pupt-flss.com/chunk-W6BLF3IL.js Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import{\$ as B,I,O as p,X as F,a as z,j as A,ja as C}from"./chunk-5J32MMV4.js";import{\$ as I,A as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-WYGBBPGQ.js Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e(isDarkTheme=new a I);isDarkTheme\$=this.isDarkTheme.asObserva", see evidence field for the suspicious	Attack	
Other Info "import{O as w}from"./chunk-5J32MMV4.js";import{d as Y}from"./chunk-GFTFIPQ3.js"; import{c as V}from"./chunk-DBNUJAAA.js";import{d", see evidence field for the suspicious comment/snippet. URL https://beta.pupt-flss.com/chunk-W6BLF3IL.js Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import{\$ as B,I,O as p,X as F,a as z,j as A,ja as C}from"./chunk-5J32MMV4.js";import{\$ as f,Aa as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-WYGBBPGQ.js Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a lnfo} for the suspicious} The suspicious of the su	Evidence	Db
Method GET Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import{\$ as B,I,O as p,X as F,a as z,j as A,ja as C}from"./chunk-5J32MMV4.js";import{\$ as f,Aa as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-WYGBBPGQ.js Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new are lnfo} 1);isDarkTheme\$=this.isDarkTheme.asObserva", see evidence field for the suspicious		"import{O as w}from"./chunk-5J32MMV4.js";import{d as Y}from"./chunk-GFTFIPQ3.js"; import{c as V}from"./chunk-DBNUJAAA.js";import{d", see evidence field for the suspicious
Attack Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import{\$ as B,I,O as p,X as F,a as z,j as A,ja as C}from"./chunk-5J32MMV4.js";import{\$ as Info f,Aa as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-WYGBBPGQ.js Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a 1);isDarkTheme\$=this.isDarkTheme.asObserva", see evidence field for the suspicious	URL	https://beta.pupt-flss.com/chunk-W6BLF3IL.js
Evidence Db The following pattern was used: \bDB\b and was detected in the element starting with: "import{\$ as B,I,O as p,X as F,a as z,j as A,ja as C}from"./chunk-5J32MMV4.js";import{\$ as f,Aa as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-WYGBBPGQ.js Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a 1);isDarkTheme\$=this.isDarkTheme.asObserva", see evidence field for the suspicious	Method	GET
The following pattern was used: \bDB\b and was detected in the element starting with: "import{\$ as B,I,O as p,X as F,a as z,j as A,ja as C}from"./chunk-5J32MMV4.js";import{\$ as f,Aa as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-WYGBBPGQ.js Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: Other "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e}isDarkTheme=new are info 1);isDarkTheme\$=this.isDarkTheme.asObserva", see evidence field for the suspicious	Attack	
Other Info "import{\$ as B,I,O as p,X as F,a as z,j as A,ja as C}from"./chunk-5J32MMV4.js";import{\$ as f,Aa as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment /snippet. URL https://beta.pupt-flss.com/chunk-WYGBBPGQ.js Method GET Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: Other import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new at 1);isDarkTheme\$=this.isDarkTheme.asObserva", see evidence field for the suspicious	Evidence	Db
Method Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: Other "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a}} 1);isDarkTheme\$=this.isDarkTheme.asObserva", see evidence field for the suspicious		"import{\$ as B,I,O as p,X as F,a as z,j as A,ja as C}from"./chunk-5J32MMV4.js";import{\$ as f,Aa as h,Cb as d,Db as b,Ga as x,Gc a", see evidence field for the suspicious comment
Attack Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: Other "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a 1);isDarkTheme\$=this.isDarkTheme.asObserva", see evidence field for the suspicious	URL	https://beta.pupt-flss.com/chunk-WYGBBPGQ.js
Evidence from The following pattern was used: \bFROM\b and was detected in the element starting with: Other "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a 1);isDarkTheme\$=this.isDarkTheme.asObserva", see evidence field for the suspicious	Method	GET
The following pattern was used: \bFROM\b and was detected in the element starting with: Other "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a}} Info 1);isDarkTheme\$=this.isDarkTheme.asObserva", see evidence field for the suspicious	Attack	
Other "import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a 1);isDarkTheme\$=this.isDarkTheme.asObserva", see evidence field for the suspicious	Evidence	from
comment/snippet.		"import{_ as s,g as a}from"./chunk-42NUSC2L.js";var m=(()=>{class e{isDarkTheme=new a(!

URL	https://beta.pupt-flss.com/chunk-YAIF3KE2.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "import{a}from"./chunk-HB25W3BE.js";import{a as n}from"./chunk-EMZRNCIP.js";import{c as s}from"./chunk-DBNUJAAA.js";import{_ as r", see evidence field for the suspicious comment/snippet.
URL	https://beta.pupt-flss.com/chunk-Z2RZOCNL.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "import{M as \$,N,a as I,d as c,e as G,f as d,r as Q}from"./chunk-5J32MMV4.js";import{d as g}from"./chunk-KA6B6XDT.js";import{\$ as", see evidence field for the suspicious comment /snippet.
URL	https://beta.pupt-flss.com/main-2UGW37G2.js
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "import{a as c}from"./chunk-PPHBMCTZ.js";import{a as H}from"./chunk-O3XO7VNM.js"; import"./chunk-YAIF3KE2.js";import{c as U,g as L", see evidence field for the suspicious comment/snippet.
Instances	29
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://beta.pupt-flss.com/
Method	GET
Attack	
Evidence	<script src="polyfills-FFHMD2TL.js" type="module"></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://beta.pupt-flss.com/login
Method	GET
Attack	
Evidence	<script src="polyfills-FFHMD2TL.js" type="module"></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://beta.pupt-flss.com/robots.txt
Method	GET
Attack	
Evidence	<script src="polyfills-FFHMD2TL.js" type="module"></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://beta.pupt-flss.com/sitemap.xml
Method	GET
Attack	
Evidence	<pre><script src="polyfills-FFHMD2TL.js" type="module"></script></pre>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	4
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109
Informational	Be evening Casha central Directives

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://beta.pupt-flss.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://beta.pupt-flss.com/sitemap.xml
Method	GET
Attack	

Evidence	
Other Info	
Instances	4
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, maxage, 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	<u>525</u>
WASC Id	13
Plugin Id	<u>10015</u>