ZAP Scanning Report - https://pomelo.fedora.tw/

Automated report generated by OWASP ZAP Automation Framework

Site: https://pomelo.fedora.tw

Generated on Thu, 29 Oct 2026 09:33:58

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	5
Low	1
Informational	3
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
SQL Injection	High	4
Absence of Anti-CSRF Tokens	Medium	Systemic
CSP: Failure to Define Directive with No Fallback	Medium	5
CSP: style-src unsafe-inline	Medium	5
Content Security Policy (CSP) Header Not Set	Medium	Systemic
Cross-Domain Misconfiguration	Medium	2
Timestamp Disclosure - Unix	Low	5
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	Systemic
Re-examine Cache-control Directives	Informational	Systemic

Alert Detail

High	SQL Injection
Description	SQL injection may be possible.
URL	https://pomelo.fedora.tw/id/forum
Node Name	https://pomelo.fedora.tw/id/forum ()(body,distro,nickname,t,title,version,website)

Method	POST
Attack	1793264634.0 ebfa213787d69b6e70381487e04a855594c0b5340a7a559cd2423384e2bb02e AND 1=1 --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [1793264634.0 ebfa213787d69b6e70381487e04a855594c0b5340a7a559cd2423384e2bb02e AND 1=1 --] and [1793264634.0 ebfa213787d69b6e70381487e04a855594c0b5340a7a559cd2423384e2bb02e AND 1=2 --] The parameter value being modified was stripped from the HTML output for the purposes of the comparison. Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.
URL	https://pomelo.fedora.tw/vi/forum
Node Name	https://pomelo.fedora.tw/vi/forum ()(body,distro,nickname,t,title,version,website)
Method	POST
Attack	1793264633.3ba4752b779e78e737b0287ebe5f16bc2d62417ae22db4605777e97152fb4fa1 AND 1=1 --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [1793264633.3 ba4752b779e78e737b0287ebe5f16bc2d62417ae22db4605777e97152fb4fa1 AND 1=1 --] and [1793264633.3 ba4752b779e78e737b0287ebe5f16bc2d62417ae22db4605777e97152fb4fa1 AND 1=2 --] The parameter value being modified was stripped from the HTML output for the purposes of the comparison. Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.
URL	https://pomelo.fedora.tw/vi/forum
Node Name	https://pomelo.fedora.tw/vi/forum ()(body,distro,nickname,t,title,version,website)
Method	POST
Attack	ZAP AND 1=1 --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [ZAP AND 1=1 --] and [ZAP AND 1=2 --] The parameter value being modified was stripped from the HTML output for the purposes of the comparison. Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.
URL	https://pomelo.fedora.tw/zh-cn/forum
Node Name	https://pomelo.fedora.tw/zh-cn/forum ()(body,distro,nickname,t,title,version,website)

Method	POST
Attack	1793264634.0 ebfa213787d69b6e70381487e04a855594c0b5340a7a559cd2423384e2bb02e AND 1=1 --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [1793264634.0 ebfa213787d69b6e70381487e04a855594c0b5340a7a559cd2423384e2bb02e AND 1=1 --] and [1793264634.0 ebfa213787d69b6e70381487e04a855594c0b5340a7a559cd2423384e2bb02e AND 1=2 --] The parameter value being modified was stripped from the HTML output for the purposes of the comparison. Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.
Instances	4
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40018

Medium	**Absence of Anti-CSRF Tokens**
	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL /form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a

Description	user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://pomelo.fedora.tw/forum
Node Name	https://pomelo.fedora.tw/forum
Method	GET
Attack	
Evidence	<form class="forum-form" method="post" action="https://pomelo.fedora.tw/forum#new">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "nickname" "t" "title" "version" "website"].
URL	https://pomelo.fedora.tw/pt-br/forum
Node Name	https://pomelo.fedora.tw/pt-br/forum
Method	GET
Attack	
Evidence	<form class="forum-form" method="post" action="https://pomelo.fedora.tw/pt-br/forum#new" >
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "nickname" "t" "title" "version" "website"].
URL	https://pomelo.fedora.tw/ru/forum
Node Name	https://pomelo.fedora.tw/ru/forum
Method	GET
Attack	
Evidence	<form class="forum-form" method="post" action="https://pomelo.fedora.tw/ru/forum#new">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "nickname" "t" "title" "version" "website"].
URL	https://pomelo.fedora.tw/th/forum
Node Name	https://pomelo.fedora.tw/th/forum
Method	GET
Attack	

Evidence	<form class="forum-form" method="post" action="https://pomelo.fedora.tw/th/forum#new">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "nickname" "t" "title" "version" "website"].
URL	https://pomelo.fedora.tw/vi/forum
Node Name	https://pomelo.fedora.tw/vi/forum
Method	GET
Attack	
Evidence	<form class="forum-form" method="post" action="https://pomelo.fedora.tw/vi/forum#new">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "nickname" "t" "title" "version" "website"].
Instances	Systemic
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	**CSP: Failure to Define Directive with No Fallback**

Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing /excluding them is the same as allowing anything.
URL	https://pomelo.fedora.tw/download/pomelo-0.34-fedora44/%E4%BD%BF%E7%94%A8%E6%89%8B%E5%86%8A.html
Node Name	https://pomelo.fedora.tw/download/pomelo-0.34-fedora44/.html
Method	GET
Attack	
Evidence	default-src 'none'; img-src 'self' data:; style-src 'unsafe-inline'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://pomelo.fedora.tw/download/pomelo-0.34-rocky9.6/%E4%BD%BF%E7%94%A8%E6%89%8B%E5%86%8A.html
Node Name	https://pomelo.fedora.tw/download/pomelo-0.34-rocky9.6/.html
Method	GET
Attack	
Evidence	default-src 'none'; img-src 'self' data:; style-src 'unsafe-inline'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://pomelo.fedora.tw/download/pomelo-0.34-ubuntu22.04/%E4%BD%BF%E7%94%A8%E6%89%8B%E5%86%8A.html
Node Name	https://pomelo.fedora.tw/download/pomelo-0.34-ubuntu22.04/.html
Method	GET
Attack	
Evidence	default-src 'none'; img-src 'self' data:; style-src 'unsafe-inline'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://pomelo.fedora.tw/download/pomelo-0.34-ubuntu24.04/%E4%BD%BF%E7%94%A8%E6%89%8B%E5%86%8A.html
Node Name	https://pomelo.fedora.tw/download/pomelo-0.34-ubuntu24.04/.html
Method	GET
Attack	
Evidence	default-src 'none'; img-src 'self' data:; style-src 'unsafe-inline'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://pomelo.fedora.tw/download/pomelo-0.34-ubuntu26.04/%E4%BD%BF%E7%94%A8%E6%89%8B%E5%86%8A.html
Node Name	https://pomelo.fedora.tw/download/pomelo-0.34-ubuntu26.04/.html
Method	GET
Attack	
Evidence	default-src 'none'; img-src 'self' data:; style-src 'unsafe-inline'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

Instances	5
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://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: style-src unsafe-inline**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://pomelo.fedora.tw/download/pomelo-0.34-fedora44/%E4%BD%BF%E7%94%A8%E6%89%8B%E5%86%8A.html
Node Name	https://pomelo.fedora.tw/download/pomelo-0.34-fedora44/.html
Method	GET
Attack	
Evidence	default-src 'none'; img-src 'self' data:; style-src 'unsafe-inline'
Other Info	style-src includes unsafe-inline.
URL	https://pomelo.fedora.tw/download/pomelo-0.34-rocky9.6/%E4%BD%BF%E7%94%A8%E6%89%8B%E5%86%8A.html
Node Name	https://pomelo.fedora.tw/download/pomelo-0.34-rocky9.6/.html
Method	GET
Attack	
Evidence	default-src 'none'; img-src 'self' data:; style-src 'unsafe-inline'
Other Info	style-src includes unsafe-inline.
URL	https://pomelo.fedora.tw/download/pomelo-0.34-ubuntu22.04/%E4%BD%BF%E7%94%A8%E6%89%8B%E5%86%8A.html
Node Name	https://pomelo.fedora.tw/download/pomelo-0.34-ubuntu22.04/.html
Method	GET
Attack	
Evidence	default-src 'none'; img-src 'self' data:; style-src 'unsafe-inline'
Other Info	style-src includes unsafe-inline.
URL	https://pomelo.fedora.tw/download/pomelo-0.34-ubuntu24.04/%E4%BD%BF%E7%94%A8%E6%89%8B%E5%86%8A.html
Node Name	https://pomelo.fedora.tw/download/pomelo-0.34-ubuntu24.04/.html

Method	GET
Attack	
Evidence	default-src 'none'; img-src 'self' data:; style-src 'unsafe-inline'
Other Info	style-src includes unsafe-inline.
URL	https://pomelo.fedora.tw/download/pomelo-0.34-ubuntu26.04/%E4%BD%BF%E7%94%A8%E6%89%8B%E5%86%8A.html
Node Name	https://pomelo.fedora.tw/download/pomelo-0.34-ubuntu26.04/.html
Method	GET
Attack	
Evidence	default-src 'none'; img-src 'self' data:; style-src 'unsafe-inline'
Other Info	style-src includes unsafe-inline.
Instances	5
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://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**Content Security Policy (CSP) Header Not Set**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://pomelo.fedora.tw/
Node Name	https://pomelo.fedora.tw/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://pomelo.fedora.tw/assistant
Node Name	https://pomelo.fedora.tw/assistant
Method	GET
Attack	
Evidence	
Other Info	

URL	https://pomelo.fedora.tw/features
Node Name	https://pomelo.fedora.tw/features
Method	GET
Attack	
Evidence	
Other Info	
URL	https://pomelo.fedora.tw/pdf
Node Name	https://pomelo.fedora.tw/pdf
Method	GET
Attack	
Evidence	
Other Info	
URL	https://pomelo.fedora.tw/project
Node Name	https://pomelo.fedora.tw/project
Method	GET
Attack	
Evidence	
Other Info	
Instances	Systemic
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	https://pomelo.fedora.tw/api/releases/latest
Node Name	https://pomelo.fedora.tw/api/releases/latest
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *

Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://pomelo.fedora.tw/api/releases/latest%EC%9D%80
Node Name	https://pomelo.fedora.tw/api/releases/latest
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	2
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://pomelo.fedora.tw/pdf
Node Name	https://pomelo.fedora.tw/pdf
Method	GET
Attack	
Evidence	1792467853
Other Info	1792467853, which evaluates to: 2026-10-20 03:44:13.
URL	https://pomelo.fedora.tw/pdf
Node Name	https://pomelo.fedora.tw/pdf
Method	GET
Attack	
Evidence	1792467859
Other Info	1792467859, which evaluates to: 2026-10-20 03:44:19.
URL	https://pomelo.fedora.tw/pdf

Node Name	https://pomelo.fedora.tw/pdf
Method	GET
Attack	
Evidence	1792467860
Other Info	1792467860, which evaluates to: 2026-10-20 03:44:20.
URL	https://pomelo.fedora.tw/pdf
Node Name	https://pomelo.fedora.tw/pdf
Method	GET
Attack	
Evidence	1792479382
Other Info	1792479382, which evaluates to: 2026-10-20 06:56:22.
URL	https://pomelo.fedora.tw/pdf
Node Name	https://pomelo.fedora.tw/pdf
Method	GET
Attack	
Evidence	1793036471
Other Info	1793036471, which evaluates to: 2026-10-26 17:41:11.
Instances	5
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://pomelo.fedora.tw/assets/site.js?v=1792479382
Node Name	https://pomelo.fedora.tw/assets/site.js (v)
Method	GET
Attack	
Evidence	edora Firefox User-Agent
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "// Ubuntu Fedora Firefox User-Agent ", see evidence field for the suspicious comment/snippet.
Instances	1
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615

WASC Id	13
Plugin Id	10027

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://pomelo.fedora.tw/
Node Name	https://pomelo.fedora.tw/
Method	GET
Attack	
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://pomelo.fedora.tw/features
Node Name	https://pomelo.fedora.tw/features
Method	GET
Attack	
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://pomelo.fedora.tw/manual
Node Name	https://pomelo.fedora.tw/manual
Method	GET
Attack	
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://pomelo.fedora.tw/pdf
Node Name	https://pomelo.fedora.tw/pdf
Method	GET
Attack	
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://pomelo.fedora.tw/project
Node Name	https://pomelo.fedora.tw/project
Method	GET
Attack	
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

Instances	Systemic
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://pomelo.fedora.tw/
Node Name	https://pomelo.fedora.tw/
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://pomelo.fedora.tw/features
Node Name	https://pomelo.fedora.tw/features
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://pomelo.fedora.tw/pdf
Node Name	https://pomelo.fedora.tw/pdf
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://pomelo.fedora.tw/robots.txt
Node Name	https://pomelo.fedora.tw/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://pomelo.fedora.tw/sitemap.xml
Node Name	https://pomelo.fedora.tw/sitemap.xml

Method	GET
Attack	
Evidence	no-cache, private
Other Info	
Instances	Systemic
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015