◈ OWASP ZAP Scan Report

Target: https://ipwija.ac.id/

All scanned sites: http://ipwija.ac.id https://pmb.ipwija.ac.id https://afiliasi.ipwija.ac.id http://repository.ipwija.ac.id https://ipwija.ac.id

Javascript included from: https://code.jquery.com https://cdnjs.cloudflare.com https://cdn.jsdelivr.net https://www.youtube-nocookie.com http://ipwija.ac.id https://pmb.ipwija.ac.id https://afiliasi.ipwija.ac.id http://repository.ipwija.ac.id https://ipwija.ac.id

Generated on Tue, 18 Nov 2025 01:42:06

ZAP Version: 2.16.1

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	9
Low	9
Informational	6

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	32
CSP: Failure to Define Directive with No Fallback	Medium	26
CSP: Wildcard Directive	Medium	26
CSP: script-src unsafe-inline	Medium	26
CSP: style-src unsafe-inline	Medium	26
Content Security Policy (CSP) Header Not Set	Medium	102
Missing Anti-clickjacking Header	Medium	102
Vulnerable JS Library	Medium	1
Weak Authentication Method	Medium	3
Big Redirect Detected (Potential Sensitive Information Leak)	Low	5
Cookie No HttpOnly Flag	Low	7
Cookie Without Secure Flag	Low	1
Cookie without SameSite Attribute	Low	1
Cross-Domain JavaScript Source File Inclusion	Low	177
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	102
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	102
Strict-Transport-Security Header Not Set	Low	102
X-Content-Type-Options Header Missing	Low	102
Authentication Request Identified	Informational	1
Charset Mismatch	Informational	44
Re-examine Cache-control Directives	Informational	102
Retrieved from Cache	Informational	102
Session Management Response Identified	Informational	7
User Controllable HTML Element Attribute (Potential XSS)	Informational	13

Passing Rules

Name	Rule Type	Threshold	Strength
Verification Request Identified	Passive	MEDIUM	-
Private IP Disclosure	Passive	MEDIUM	-
Session ID in URL Rewrite	Passive	MEDIUM	-
Script Served From Malicious Domain (polyfill)	Passive	MEDIUM	-
ZAP is Out of Date	Passive	MEDIUM	-
Insecure JSF ViewState	Passive	MEDIUM	-
Content-Type Header Missing	Passive	MEDIUM	-
Application Error Disclosure	Passive	MEDIUM	-
Information Disclosure - Debug Error Messages	Passive	MEDIUM	-
Information Disclosure - Sensitive Information in URL	Passive	MEDIUM	-
Information Disclosure - Sensitive Information in HTTP Referrer Header	Passive	MEDIUM	-
Information Disclosure - Suspicious Comments	Passive	MEDIUM	-

[Off-site Redirect](#)	Passive	MEDIUM	-
[Cookie Poisoning](#)	Passive	MEDIUM	-
[User Controllable Charset](#)	Passive	MEDIUM	-
[WSDL File Detection](#)	Passive	MEDIUM	-
[Loosely Scoped Cookie](#)	Passive	MEDIUM	-
[Viewstate](#)	Passive	MEDIUM	-
[Directory Browsing](#)	Passive	MEDIUM	-
[Heartbleed OpenSSL Vulnerability (Indicative)](#)	Passive	MEDIUM	-
[X-Backend-Server Header Information Leak](#)	Passive	MEDIUM	-
[Secure Pages Include Mixed Content](#)	Passive	MEDIUM	-
[HTTP to HTTPS Insecure Transition in Form Post](#)	Passive	MEDIUM	-
[HTTPS to HTTP Insecure Transition in Form Post](#)	Passive	MEDIUM	-
[User Controllable JavaScript Event (XSS)](#)	Passive	MEDIUM	-
[X-ChromeLogger-Data (XCOLD) Header Information Leak](#)	Passive	MEDIUM	-
[X-Debug-Token Information Leak](#)	Passive	MEDIUM	-
[Username Hash Found](#)	Passive	MEDIUM	-
[X-AspNet-Version Response Header](#)	Passive	MEDIUM	-
[PII Disclosure](#)	Passive	MEDIUM	-
[Script Passive Scan Rules](#)	Passive	MEDIUM	-
[Stats Passive Scan Rule](#)	Passive	MEDIUM	-
[Timestamp Disclosure](#)	Passive	MEDIUM	-
[Hash Disclosure](#)	Passive	MEDIUM	-
[Cross-Domain Misconfiguration](#)	Passive	MEDIUM	-
[Reverse Tabnabbing](#)	Passive	MEDIUM	-
[Modern Web Application](#)	Passive	MEDIUM	-

Alert Detail

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://repository.ipwija.ac.id/cgi/register
Method	GET
Parameter	
Attack	
Evidence	<form method="post" accept-charset="utf-8" action="/cgi/register" enctype="multipart/form-data">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 2: "_action_register" "_default_action" "c1_name_family" "c1_name_given" "c1_name_honourific" "c1_newemail" "c1_newpassword" "c1_username" "screen"].
Request Header	GET http://repository.ipwija.ac.id/cgi/register HTTP/1.1 host: repository.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: http://repository.ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:38:12 GMT Server: Apache/2.4.29 (Ubuntu) Cache-Control: no-store, no-cache, must-revalidate Vary: Accept-Encoding Content-Type: text/html; charset=utf-8 content-length: 9656
Response Body **(excerpt)**	irmation email will be sent to you. You need to activate your account using the link in the email.</p> <p>If you have already registered but have forgotten your username or password, click here to set a new password.</p> **<form method="post" accept-charset="utf-8" action="/cgi/register" enctype="multipart/form-data">**<input name="screen" id="screen" value="Register::Internal" type="hidden" /><div class="ep_form_field_input"><div class="ep_sr_none"><table cl
URL	http://repository.ipwija.ac.id/cgi/reset_password

Method	GET
Parameter	
Attack	
Evidence	<form method="post" accept-charset="utf-8" action="reset_password" enctype="multipart/form-data">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 2: "_action_submit" "_default" "_default_action" "email" "newpassword"].
URL	http://repository.ipwija.ac.id/policies.html
Method	GET
Parameter	
Attack	
Evidence	<form method="post" action="http://www.opendoar.org/tools/policytool.php">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 2: "la" "rOaiBaseUrl" "rUrl"].
URL	https://ipwija.ac.id/events/ujian-tengah-semester-ganjil/
Method	GET
Parameter	
Attack	
Evidence	<form action="https://ipwija.ac.id/wp-comments-post.php" method="post" id="commentform" class="comment-form" novalidate>
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "author" "comment_parent" "comment_post_ID" "email" "g-recaptcha-response" "submit" "url"].
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	<form id="form_filter" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "act"].
URL	https://pmb.ipwija.ac.id/?lang=en
Method	GET
Parameter	
Attack	
Evidence	<form id="form_filter" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "act"].
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	
Attack	
Evidence	<form id="form_filter" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "act"].
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	
Attack	
Evidence	<form id="form_filter" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "act"].
URL	https://pmb.ipwija.ac.id/home?lang=en
Method	GET
Parameter	
Attack	
Evidence	<form id="form_filter" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "act"].
URL	https://pmb.ipwija.ac.id/home?lang=id
Method	GET
Parameter	
Attack	
Evidence	<form id="form_filter" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "act"].
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET

Parameter	
Attack	
Evidence	\<form method="post"\>
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 10: ""].
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	
Attack	
Evidence	\<form method="post"\>
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: ""].
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	
Attack	
Evidence	\<form method="post"\>
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 2: "act" "kampus" "key" "key_unit"].
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	
Attack	
Evidence	\<form method="post"\>
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 3: "act" "kampus" "key" "key_unit"].
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	
Attack	
Evidence	\<form method="post"\>
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 4: "act" "kampus" "key" "key_unit"].
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	
Attack	
Evidence	\<form method="post"\>
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 5: "act" "kampus" "key" "key_unit"].
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	
Attack	
Evidence	\<form method="post"\>
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 6: "act" "kampus" "key" "key_unit"].
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	
Attack	
Evidence	\<form method="post"\>
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 7: "act" "kampus" "key" "key_unit"].
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	
Attack	
Evidence	\<form method="post"\>
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 8: "act" "kampus" "key" "key_unit"].
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	

Attack	
Evidence	<form method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 9: "act"].
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	
Attack	
Evidence	<form name="pageform" id="pageform" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "act" "page"].
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/15401
Method	GET
Parameter	
Attack	
Evidence	<form action="/jalur-seleksi" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "act" "key" "prodipilihan"].
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/15401
Method	GET
Parameter	
Attack	
Evidence	<form action="/jalur-seleksi" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 2: "act" "key" "prodipilihan"].
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/15401
Method	GET
Parameter	
Attack	
Evidence	<form action="/jalur-seleksi" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 3: "act" "key" "prodipilihan"].
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/61101
Method	GET
Parameter	
Attack	
Evidence	<form action="/jalur-seleksi" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "act" "key" "prodipilihan"].
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/61101
Method	GET
Parameter	
Attack	
Evidence	<form action="/jalur-seleksi" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 2: "act" "key" "prodipilihan"].
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/61101
Method	GET
Parameter	
Attack	
Evidence	<form action="/jalur-seleksi" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 3: "act" "key" "prodipilihan"].
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/61101
Method	GET
Parameter	
Attack	
Evidence	<form action="/jalur-seleksi" method="post">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 4: "act" "key" "prodipilihan"].
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/61201
Method	GET
Parameter	
Attack	

Evidence	`<form action="/jalur-seleksi" method="post">`
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "act" "key" "prodipilihan"].
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/61201
Method	GET
Parameter	
Attack	
Evidence	`<form action="/jalur-seleksi" method="post">`
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 2: "act" "key" "prodipilihan"].
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/61201
Method	GET
Parameter	
Attack	
Evidence	`<form action="/jalur-seleksi" method="post">`
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 3: "act" "key" "prodipilihan"].
URL	http://repository.ipwija.ac.id/cgi/register
Method	POST
Parameter	
Attack	
Evidence	`<form method="post" accept-charset="utf-8" action="/cgi/register" enctype="multipart/form-data">`
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 2: "_action_register" "_default_action" "c1_name_family" "c1_name_given" "c1_name_honourific" "c1_newemail" "c1_newpassword" "c1_username" "screen"].
Instances	32
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://ipwija.ac.id/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

Request Header	`GET https://ipwija.ac.id/ HTTP/1.1`
	`host: ipwija.ac.id`
	`user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36`
	`pragma: no-cache`
	`cache-control: no-cache`

Request Body	

| Response Header | ```
HTTP/1.1 200 OK
Date: Tue, 18 Nov 2025 01:36:07 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/8.2.28
Link: <https://ipwija.ac.id/wp-json/>; rel="https://api.w.org/"
Link: <https://ipwija.ac.id/wp-json/wp/v2/pages/15509>; rel="alternate"; title="JSON"; type="application/json"
Link: <https://ipwija.ac.id/>; rel=shortlink
Etag: W/"99-1762975106;gz"
X-LiteSpeed-Cache: hit
platform: hostinger
panel: hpanel
Content-Security-Policy: upgrade-insecure-requests
Age: 526
Server: hcdn
alt-svc: h3=":443"; ma=86400
x-hcdn-request-id: 1c7fc13d5ff49deccd08f5a201f8b8f8-bos-edge4
x-hcdn-cache-status: HIT
content-length: 415329
``` |
| Response Body **(truncated)** | ```
<!DOCTYPE html>
<html itemscope itemtype="http://schema.org/WebPage" lang="en-US">
<head>
        <meta charset="UTF-8">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="profile" href="http://gmpg.org/xfn/11">
        <link rel="pingback" href="https://ipwija.ac.id/xmlrpc.php">
        <title>Universitas IPWIJA &#8211; Universitas IPWIJA</title>
<style>
#wpadminbar #wp-admin-bar-wsm_free_top_button .ab-icon:before {
        content: "\f239";
        color: #FF9800;
        top: 3px;
}
</style><meta name=...(truncated)
``` |

URL	https://ipwija.ac.id/aktivitas/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/biaya-kuliah-universitas-ipwija/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/events/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/fasilitas/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/home/u329130267/domains/ipwija.ac.id/public_html/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/informasi-beasiswa/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

URL	https://ipwija.ac.id/informasi-tes-seleksi/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/kemahasiswaan/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/keseharian-di-kampus/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/klinik/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/lembaga-sertifikasi-profesi
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/magister-manajemen/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/pendaftaran/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/pengumuman-penerimaan/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/perpustakaan/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/program-studi-informatika/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

URL	https://ipwija.ac.id/program-studi-kewirausahaan/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/program-studi-rekayasa-perangkat-lunak/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/program-studi-sistem-informasi/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/pusat-konseling/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/pusat-teknologi-informasi/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/simulasi-rapor/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/tanggal-penting/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ipwija.ac.id/tentang-universitas-ipwija/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
Instances	26
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: 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://ipwija.ac.id/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
Request Header	GET https://ipwija.ac.id/ HTTP/1.1 host: ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:07 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Vary: Accept-Encoding X-Powered-By: PHP/8.2.28 Link: <https://ipwija.ac.id/wp-json/>; rel="https://api.w.org/" Link: <https://ipwija.ac.id/wp-json/wp/v2/pages/15509>; rel="alternate"; title="JSON"; type="application/json" Link: <https://ipwija.ac.id/>; rel=shortlink Etag: W/"99-1762975106;gz" X-LiteSpeed-Cache: hit platform: hostinger panel: hpanel Content-Security-Policy: **upgrade-insecure-requests** Age: 526 Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 1c7fc13d5ff49deccd08f5a201f8b8f8-bos-edge4 x-hcdn-cache-status: HIT content-length: 415329

Response Body **(truncated)**	<!DOCTYPE html>
	<html itemscope itemtype="http://schema.org/WebPage" lang="en-US">
	<head>
	    <meta charset="UTF-8">
	    <meta name="viewport" content="width=device-width, initial-scale=1">
	    <link rel="profile" href="http://gmpg.org/xfn/11">
	    <link rel="pingback" href="https://ipwija.ac.id/xmlrpc.php">
	    <title>Universitas IPWIJA – Universitas IPWIJA</title>
	<style>
	#wpadminbar #wp-admin-bar-wsm_free_top_button .ab-icon:before {
	    content: "\f239";
	    color: #FF9800;
	    top: 3px;
	}
	</style><meta name=...(truncated)

URL	https://ipwija.ac.id/aktivitas/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/biaya-kuliah-universitas-ipwija/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/events/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/fasilitas/

Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/home/u329130267/domains/ipwija.ac.id/public_html/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/informasi-beasiswa/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/informasi-tes-seleksi/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/kemahasiswaan/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/keseharian-di-kampus/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/klinik/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/lembaga-sertifikasi-profesi
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/magister-manajemen/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/pendaftaran/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/pengumuman-penerimaan/

Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/perpustakaan/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/program-studi-informatika/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/program-studi-kewirausahaan/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/program-studi-rekayasa-perangkat-lunak/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/program-studi-sistem-informasi/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/pusat-konseling/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/pusat-teknologi-informasi/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/simulasi-rapor/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/tanggal-penting/

Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
URL	https://ipwija.ac.id/tentang-universitas-ipwija/
Method	GET
Parameter	Content-Security-Policy
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, font-src, media-src, object-src, manifest-src, worker-src
Instances	26
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: 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://ipwija.ac.id/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
Request Header	GET https://ipwija.ac.id/ HTTP/1.1 host: ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:07 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Vary: Accept-Encoding X-Powered-By: PHP/8.2.28 Link: <https://ipwija.ac.id/wp-json/>; rel="https://api.w.org/" Link: <https://ipwija.ac.id/wp-json/wp/v2/pages/15509>; rel="alternate"; title="JSON"; type="application/json" Link: <https://ipwija.ac.id/>; rel=shortlink Etag: W/"99-1762975106;gz" X-LiteSpeed-Cache: hit platform: hostinger panel: hpanel Content-Security-Policy: **upgrade-insecure-requests** Age: 526 Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 1c7fc13d5ff49deccd08f5a201f8b8f8-bos-edge4 x-hcdn-cache-status: HIT content-length: 415329

Response Body **(truncated)**	`<!DOCTYPE html>`
	`<html itemscope itemtype="http://schema.org/WebPage" lang="en-US">`
	`<head>`
	`        <meta charset="UTF-8">`
	`        <meta name="viewport" content="width=device-width, initial-scale=1">`
	`        <link rel="profile" href="http://gmpg.org/xfn/11">`
	`        <link rel="pingback" href="https://ipwija.ac.id/xmlrpc.php">`
	`        <title>Universitas IPWIJA – Universitas IPWIJA</title>`
	`<style>`
	`#wpadminbar #wp-admin-bar-wsm_free_top_button .ab-icon:before {`
	`        content: "\f239";`
	`        color: #FF9800;`
	`        top: 3px;`
	`}`
	`</style><meta name=...(truncated)`

URL	https://ipwija.ac.id/aktivitas/
Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/biaya-kuliah-universitas-ipwija/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/events/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/fasilitas/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/home/u329130267/domains/ipwija.ac.id/public_html/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/informasi-beasiswa/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/informasi-tes-seleksi/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/kemahasiswaan/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/keseharian-di-kampus/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/klinik/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/lembaga-sertifikasi-profesi
Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/magister-manajemen/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/pendaftaran/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/pengumuman-penerimaan/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/perpustakaan/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/program-studi-informatika/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/program-studi-kewirausahaan/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/program-studi-rekayasa-perangkat-lunak/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/program-studi-sistem-informasi/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/pusat-konseling/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/pusat-teknologi-informasi/
Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/simulasi-rapor/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/tanggal-penting/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://ipwija.ac.id/tentang-universitas-ipwija/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
Instances	26
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://ipwija.ac.id/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
Request Header	GET https://ipwija.ac.id/ HTTP/1.1 host: ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:07 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Vary: Accept-Encoding X-Powered-By: PHP/8.2.28 Link: <https://ipwija.ac.id/wp-json/>; rel="https://api.w.org/" Link: <https://ipwija.ac.id/wp-json/wp/v2/pages/15509>; rel="alternate"; title="JSON"; type="application/json" Link: <https://ipwija.ac.id/>; rel=shortlink Etag: W/"99-1762975106;gz" X-LiteSpeed-Cache: hit platform: hostinger panel: hpanel Content-Security-Policy: **upgrade-insecure-requests**

Age: 526
Server: hcdn
alt-svc: h3=":443"; ma=86400
x-hcdn-request-id: 1c7fc13d5ff49deccd08f5a201f8b8f8-bos-edge4
x-hcdn-cache-status: HIT
content-length: 415329

| Response Body **(truncated)** | ```<!DOCTYPE html>
<html itemscope itemtype="http://schema.org/WebPage" lang="en-US">
<head>
        <meta charset="UTF-8">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="profile" href="http://gmpg.org/xfn/11">
        <link rel="pingback" href="https://ipwija.ac.id/xmlrpc.php">
        <title>Universitas IPWIJA – Universitas IPWIJA</title>
<style>
#wpadminbar #wp-admin-bar-wsm_free_top_button .ab-icon:before {
        content: "\f239";
        color: #FF9800;
        top: 3px;
}
</style><meta name=...(truncated)``` |
| --- | --- |

URL	https://ipwija.ac.id/aktivitas/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/biaya-kuliah-universitas-ipwija/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/events/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/fasilitas/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/home/u329130267/domains/ipwija.ac.id/public_html/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/informasi-beasiswa/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/informasi-tes-seleksi/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/kemahasiswaan/
Method	GET
Parameter	Content-Security-Policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/keseharian-di-kampus/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/klinik/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/lembaga-sertifikasi-profesi
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/magister-manajemen/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/pendaftaran/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/pengumuman-penerimaan/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/perpustakaan/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/program-studi-informatika/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/program-studi-kewirausahaan/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/program-studi-rekayasa-perangkat-lunak/
Method	GET
Parameter	Content-Security-Policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/program-studi-sistem-informasi/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/pusat-konseling/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/pusat-teknologi-informasi/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/simulasi-rapor/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/tanggal-penting/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://ipwija.ac.id/tentang-universitas-ipwija/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
Instances	26
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	http://repository.ipwija.ac.id/
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
Request Header	GET http://repository.ipwija.ac.id/ HTTP/1.1 host: repository.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:10 GMT Server: Apache/2.4.29 (Ubuntu) Expires: Thu, 18 Dec 2025 01:36:10 GMT Cache-Control: no-store, no-cache, must-revalidate Vary: Accept-Encoding Content-Type: text/html; charset=utf-8 content-length: 8178
Response Body **(truncated)**	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="X-UA-Compatible" content="IE=edge" /> <title>Welcome to UNIVERSITAS IPWIJA Repository - UNIVERSITAS IPWIJA REPOSITORY</title> <link rel="icon" href="/favicon.ico" type="image/x-icon" /> <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" /> <link rel="alternate" type="...(truncated)
URL	http://repository.ipwija.ac.id/cgi/latest
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/cgi/register
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/cgi/search/advanced
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/cgi/users/home
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/eprints/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/id/contents
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/information.html
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/policies.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/sword-app/servicedocument
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/creators/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/creators/index.B.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/fac=5Feng/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/fac=5Flaw/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/fac=5Fmed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fart/
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fecs/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fedu/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fman/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fmat/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fmed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fsoc/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/A.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/AC.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/AI.html
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/AS.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/B.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/BF.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/H.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/H1.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HB.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HC.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HD.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HD28.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HD61.html
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HG.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HJ.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HN.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HV.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/L.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/LB.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/LB2361.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/Q.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/Q1.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/QA.html
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/QA75.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/subjects.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/0031.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/1998.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/1999.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2001.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2004.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2005.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2006.html
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2008.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2009.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2010.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2011.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2012.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2013.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2014.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2015.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2016.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2017.html
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2018.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2019.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2020.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2021.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2022.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2023.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2024.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2025.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/NULL.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/uploads/2024/10/illustrasi-sarjana-manajemen.jpg
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/uploads/2025/04/Frame-695-1024x1536.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/uploads/2025/04/Frame-695-200x300.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/uploads/2025/04/Frame-695-683x1024.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/uploads/2025/04/Frame-695-768x1152.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/uploads/2025/04/Frame-695.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=en
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/detail-pengumuman/3/brosur-pmb-20252026
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/home?lang=en
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/home?lang=id
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/15401
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/55201
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/57201
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/59202
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/61101
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/61201
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/94202
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/user-guide
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	102
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	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	http://repository.ipwija.ac.id/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
Request Header	GET http://repository.ipwija.ac.id/ HTTP/1.1 host: repository.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:10 GMT Server: Apache/2.4.29 (Ubuntu) Expires: Thu, 18 Dec 2025 01:36:10 GMT Cache-Control: no-store, no-cache, must-revalidate Vary: Accept-Encoding Content-Type: text/html; charset=utf-8 content-length: 8178
Response Body **(truncated)**	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml">

```
  <head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <title>Welcome to UNIVERSITAS IPWIJA Repository  - UNIVERSITAS IPWIJA REPOSITORY</title>
    <link rel="icon" href="/favicon.ico" type="image/x-icon" />
    <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" />

    <link rel="alternate" type="...(truncated)
```

URL	http://repository.ipwija.ac.id/cgi/latest
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/cgi/register
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/cgi/search/advanced
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/eprints/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/information.html
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/policies.html
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/creators/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://afiliasi.ipwija.ac.id/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://afiliasi.ipwija.ac.id/login
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://afiliasi.ipwija.ac.id/register
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/aktivitas/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/aktivitas/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/alumni-2/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/arsip/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/author/uipwija-2/
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/banjir-di-bekasi-civitas-ipwija-gotong-royong-pulihkan-lingkungan/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/bem-universitas-ipwija-sukses-gelar-iscom-2025-ajang-kompetisi-olahraga-penuh-semangat/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/berita/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/biaya-kuliah-universitas-ipwija/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/biaya-kuliah-universitas-ipwija/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/bu/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/category/berita-kampus/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/category/kegiatan-mahasiswa/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/pengisian-krs-genap-2025-2026/
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/pengumuman-khs-semester-ganjil/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/perkuliahan-semester-ganjil-2025-2026/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/uji-kompetensi-lsp/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/ujian-akhir-semester-ganjil-uas/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/ujian-tengah-semester-ganjil/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/wisuda/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/yudisium/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/fasilitas/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/hubungi-kami/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/ija-ppkd-jakarta-utara-gelar-pelatihan-cyber-security-untuk-tingkatkan-kompetensi-digital/
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/inagurasi-mahasiswa-baru-kampus-universitas-ipwija-2024-home-happy-orientation-motivation-education/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/informasi-beasiswa/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/informasi-tes-seleksi/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/informasi-tes-seleksi/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/ipwija-pemkot-bekasi-wujudkan-asn-dan-masyarakat-adaptif-lewat-pelatihan-public-speaking-ai-content-creator/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/kabar-terbaru/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/kebijakan-dan-pengumuman/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/kemahasiswaan/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/keseharian-di-kampus/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/keseharian-di-kampus/embed/
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/klinik/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/lembaga-sertifikasi-profesi/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/lowongan-pekerjaan-simgroup-career-day-bekasi/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/lowongan-pekerjaan/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/lowongan-posisi-strategis-di-perusahaan-startup-pasar-modal/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/magister-manajemen/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/marina-goes-to-school-campus-di-universitas-ipwija-no-limit-under-the-sun/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/mengapa-ipwija/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pemanfaatan-ai-dalam-wirausaha-universitas-ipwija-gelar-sharing-session/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/penandatanganan-mou-dan-pks-universitas-ipwija-dengan-pt-lima-sekawan-indonesia-hive-five/
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pendaftaran/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pengumuman-penerimaan/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pentas-seni-universitas-ipwija-2025-youthful-rhapsody-kebebasan-berekspresi/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/perpustakaan/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-informatika/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-kebidanan/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-kewirausahaan/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-rekayasa-perangkat-lunak/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-sarajana-manajemen/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-sistem-informasi/
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pusat-karir/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pusat-konseling/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pusat-teknologi-informasi/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/sekilas-ipwija/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/seleksi-penerimaan-pendidikan-calon-pegawai-pcp-angkatan-ke-5/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/silaturahmi-pascalebaran-universitas-ipwija-gelar-halal-bihalal-bersama-pimpinan-yayasan-dan-universitas/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/simulasi-rapor/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/sorotan/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/sosialisasi-p2mw-2025-di-universitas-ipwija-mahasiswa-didorong-jadi-wirausahawan-muda/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/tanggal-penting-pendaftaran/
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/tanggal-penting/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/tanggal-penting/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/tentang-universitas-ipwija/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/video/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=en
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/detail-pengumuman/3/brosur-pmb-20252026
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/15401
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/55201
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/57201
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/59202
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/61101
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/61201
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi-detail/detail/94202
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/user-guide
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
Instances	102
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	Vulnerable JS Library
Description	The identified library appears to be vulnerable.
URL	https://ipwija.ac.id/wp-content/themes/eduma/assets/js/main.min.js?ver=5.6.6
Method	GET
Parameter	
Attack	
Evidence	* Bootstrap v3.2.0
Other Info	The identified library bootstrap, version 3.2.0 is vulnerable. CVE-2018-14041 CVE-2019-8331 CVE-2018-20677 CVE-2018-20676 CVE-2018-14042 CVE-2016-10735 CVE-2024-6485 https://nvd.nist.gov/vuln/detail/CVE-2024-6485 https://github.com/twbs/bootstrap/issues/28236 https://www.herodevs.com/vulnerability-directory/cve-2024-6485 https://github.com/advisories/GHSA-pj7m-g53m-7638 https://github.com/twbs/bootstrap/issues/20184 https://github.com/advisories/GHSA-vxmc-5x29-h64v https://github.com/advisories/GHSA-ph58-4vrj-w6hr https://github.com/twbs/bootstrap https://github.com/twbs/bootstrap/issues/20631 https://github.com/advisories/GHSA-4p24-vmcr-4gqj https://github.com/advisories/GHSA-9v3m-8fp8-mj99 https://nvd.nist.gov/vuln/detail/CVE-2018-20676
Request Header	GET https://ipwija.ac.id/wp-content/themes/eduma/assets/js/main.min.js?ver=5.6.6 HTTP/1.1 host: ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:14 GMT Content-Type: application/x-javascript Connection: keep-alive Vary: Accept-Encoding Cache-Control: public, max-age=604800 Expires: Tue, 25 Nov 2025 01:36:14 GMT Last-Modified: Fri, 14 Mar 2025 15:38:09 GMT Etag: W/"13a3a-67d44d61-c4223ab12e0473e8;gz" platform: hostinger panel: hpanel Content-Security-Policy: upgrade-insecure-requests Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 3e3483e35ea58f0792f5a722ee8dbbd8-bos-edge1 x-hcdn-cache-status: MISS x-hcdn-upstream-rt: 0.786 content-length: 80442

Response Body **(excerpt)**	/* CONTENT:
	 - bootstrap from thimframework
	  - Owl carousel
	  - jQuery Cookie
	 - theia-sticky-sidebar
	  */
	
	/**
	 * Bootstrap v3.2.0 (http://getbootstrap.com) - Copy from thim-framework
	 * Copyright 2011-2014 Twitter, Inc.
	 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
	 */
	if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript require

Instances	1
Solution	Upgrade to the latest version of the affected library.
Reference	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
CWE Id	1395
WASC Id	

Plugin Id		[10003](#)

Medium	Weak Authentication Method
Description	HTTP basic or digest authentication has been used over an unsecured connection. The credentials can be read and then reused by someone with access to the network.

URL	http://repository.ipwija.ac.id/cgi/users/home
Method	GET
Parameter	
Attack	
Evidence	www-authenticate: Basic realm="UNIVERSITAS IPWIJA REPOSITORY"
Other Info	
Request Header	GET http://repository.ipwija.ac.id/cgi/users/home HTTP/1.1 host: repository.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: http://repository.ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 401 Unauthorized Date: Tue, 18 Nov 2025 01:38:11 GMT Server: Apache/2.4.29 (Ubuntu) WWW-Authenticate: Basic realm="UNIVERSITAS IPWIJA REPOSITORY" Content-Length: 470 Content-Type: text/html; charset=iso-8859-1
Response Body	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <html><head> <title>401 Unauthorized</title> </head><body> Unauthorized This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required. <hr> <address>Apache/2.4.29 (Ubuntu) Server at repository.ipwija.ac.id Port 80</address> </body></html>
URL	http://repository.ipwija.ac.id/id/contents
Method	GET
Parameter	
Attack	
Evidence	www-authenticate: Basic realm="UNIVERSITAS IPWIJA REPOSITORY"
Other Info	
URL	http://repository.ipwija.ac.id/sword-app/servicedocument
Method	GET
Parameter	
Attack	
Evidence	www-authenticate: Basic realm="UNIVERSITAS IPWIJA REPOSITORY"
Other Info	
Instances	3
Solution	Protect the connection using HTTPS or use a stronger authentication mechanism.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
CWE Id	[326](#)
WASC Id	4
Plugin Id	[10105](#)

Low	Big Redirect Detected (Potential Sensitive Information Leak)
Description	The server has responded with a redirect that seems to provide a large response. This may indicate that although the server sent a redirect it also responded with body content (which may include sensitive details, PII, etc.).

URL	http://ipwija.ac.id/informasi-beasiswa/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	Location header URI length: 40 [https://ipwija.ac.id/informasi-beasiswa/]. Predicted response size: 340. Response Body Length: 795.
Request Header	GET http://ipwija.ac.id/informasi-beasiswa/ HTTP/1.1 host: ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache

	cache-control: no-cache referer: https://ipwija.ac.id/pendaftaran/
Request Body	
Response Header	HTTP/1.1 301 Moved Permanently Date: Tue, 18 Nov 2025 01:37:05 GMT Content-Type: text/html Content-Length: 795 Connection: keep-alive Location: https://ipwija.ac.id/informasi-beasiswa/ platform: hostinger panel: hpanel Content-Security-Policy: upgrade-insecure-requests Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 4c5cf0770a224be003819b206f949d3f-bos-edge5 x-hcdn-cache-status: MISS x-hcdn-upstream-rt: 0.501
Response Body **(truncated)**	<!DOCTYPE html> <html style="height:100%"> <head> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /> <title> 301 Moved Permanently </title><style>@media (prefers-color-scheme:dark){body{background-color:#000!important}}</style></head> <body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> <div style="height:auto; min-height:100%; "> <div style="text-align: center; width:800px; margi...(truncated)
URL	http://repository.ipwija.ac.id/cgi/search/advanced? _action_newsearch=Reset+the+form&abstract=ZAP&abstract_merge=ALL&creators_name=ZAP&creators_name_merge=ALL&dataset=archive&date=ZAP&department=ZAP&department_merge=ALL&documents=ZAP&documents.format=text&documents_merge=ALL date%2Fcreators_name%2Ftitle&publication=ZAP&publication_merge=ALL&refereed=EITHER&satisfyall=ALL&screen=Search&subjects=AC&subjects_merge=ANY&title=ZAP&title_merge=ALL&type=article
Method	GET
Parameter	
Attack	
Evidence	
Other Info	Location header URI length: 529 [/cgi/search/archive/advanced? _action_newsearch=Reset+the+form&abstract=ZAP&abstract_merge=ALL&creators_name=ZAP&creators_name_merge=ALL&dataset=archive&date=ZAP&department=ZAP&department_merge=ALL&documents=ZAP&documents.format=text&documents_merge=ALL date%2Fcreators_name%2Ftitle&publication=ZAP&publication_merge=ALL&refereed=EITHER&satisfyall=ALL&screen=Search&subjects=AC&subjects_merge=ANY&title=ZAP&title_merge=ALL&type=article]. Predicted response size: 829. Response Body Length: 910
URL	http://repository.ipwija.ac.id/cgi/search/advanced? _action_search=Search&abstract=ZAP&abstract_merge=ALL&creators_name=ZAP&creators_name_merge=ALL&dataset=archive&date=ZAP&department=ZAP&department_merge=ALL&documents=ZAP&documents.format=text&documents_merge=ALL&editors_na date%2Fcreators_name%2Ftitle&publication=ZAP&publication_merge=ALL&refereed=EITHER&satisfyall=ALL&screen=Search&subjects=AC&subjects_merge=ANY&title=ZAP&title_merge=ALL&type=article
Method	GET
Parameter	
Attack	
Evidence	
Other Info	Location header URI length: 518 [/cgi/search/archive/advanced? _action_search=Search&abstract=ZAP&abstract_merge=ALL&creators_name=ZAP&creators_name_merge=ALL&dataset=archive&date=ZAP&department=ZAP&department_merge=ALL&documents=ZAP&documents.format=text&documents_merge=ALL&editors_na date%2Fcreators_name%2Ftitle&publication=ZAP&publication_merge=ALL&refereed=EITHER&satisfyall=ALL&screen=Search&subjects=AC&subjects_merge=ANY&title=ZAP&title_merge=ALL&type=article]. Predicted response size: 818. Response Body Length: 899
URL	https://afiliasi.ipwija.ac.id/storeRegister
Method	POST
Parameter	
Attack	
Evidence	
Other Info	Location header URI length: 38 [https://afiliasi.ipwija.ac.id/register]. Predicted response size: 338. Response Body Length: 398.
URL	https://afiliasi.ipwija.ac.id/validateLogin
Method	POST
Parameter	
Attack	
Evidence	
Other Info	Location header URI length: 35 [https://afiliasi.ipwija.ac.id/login]. Predicted response size: 335. Response Body Length: 386.
Instances	5
Solution	Ensure that no sensitive information is leaked via redirect responses. Redirect responses should have almost no content.
Reference	
CWE Id	201
WASC Id	13
Plugin Id	10044

Low	Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://afiliasi.ipwija.ac.id/
Method	GET
Parameter	XSRF-TOKEN
Attack	

Evidence	set-cookie: XSRF-TOKEN
Other Info	
Request Header	GET https://afiliasi.ipwija.ac.id/ HTTP/1.1 host: afiliasi.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:10 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Vary: Accept-Encoding X-Powered-By: PHP/8.2.28 Cache-Control: no-cache, private **set-cookie: XSRF-TOKEN**=eyJpdiI6IkRWL2pDSXRIVVJLNndZalVobGpkeWc9PSIsInZhbHVlIjoiMjkxV2hQM09NL21YTHZaN2FJLzc3c0VqVzZHSnVxUVMzYmFQVndScnl4Rm1qZGlSUXZtNi9KdnFabjhMbHpNRkF1V2VwdmNxd3ZhaWJVaUVPZlZHRiswK3VTenBPZ2NMT3JhSGVzeFY3RTZ2Vy9OZ01LSEhBbFRTelU1eHlCTFUiLCJtYWMiOiJlZjM3Mzk1NTBlZjdiNjRjYTlhYzVlMDZmYWZiMzIwNWVjNzY1ZjRiNDJhYmFiMmU3ZWMxZTkzNGE1ZDc3ZWNjIiwidGFnIjoiIn0%3D; expires=Tue, 18 Nov 2025 03:36:10 GMT; Max-Age=7200; path=/; secure; samesite=lax set-cookie: laravel_session=eyJpdiI6ImJvVkZqRExGd0hvWXdsZm04bklOVkE9PSIsInZhbHVlIjoiUkpWbmk1aE03TmVlbTg1MTQvMHVGcG0vMUZrRlpMQ2Y3cWx5a29adkpWS0l2VmZDRjdheE9FMHp0NFNKb0F5K0VlWDltOHdnU3FqTGd6Ym9kbDEvRDRiOGVicVdKR2M4ejlCSDAwanloSzVkZ0oyU0lmS2psOXJDQmp4b3F3VTQiLCJtYWMiOiI1NzhkNzQ2MjY3NDNmYWNhNTk0MmJhMjFlMmQ2YjBlYTBmNWJmOTZlMDk1MzI1ZTQ5NjUxNmRjZTJJkYzJiNDQ5IiwidGFnIjoiIn0%3D; expires=Tue, 18 Nov 2025 03:36:10 GMT; Max-Age=7200; path=/; secure; httponly; samesite=lax platform: hostinger panel: hpanel Content-Security-Policy: upgrade-insecure-requests Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 4f489f24ae6ec7bc0e1d96f5bc550939-bos-edge4 x-hcdn-cache-status: DYNAMIC x-hcdn-upstream-rt: 0.825 content-length: 32839

Response Body **(truncated)**	`<!DOCTYPE html>`
	`<html lang="en">`
	
	`<head>`
	`    <meta charset="UTF-8">`
	`    <meta name="viewport" content="width=device-width, initial-scale=1.0">`
	`    <title>Program Afiliasi IPWIJA</title>`
	`    <!-- Bootstrap CSS -->`
	`    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">`
	`    <link rel="preconnect" href="https://fonts.googleapis.com">`
	`    <link rel="preconnect" href="https://fonts.gstatic.com" crossorigin>`
	`    <link href="https://fonts.go...(truncated)`

URL	https://afiliasi.ipwija.ac.id/forgot-password
Method	GET
Parameter	XSRF-TOKEN
Attack	
Evidence	set-cookie: XSRF-TOKEN
Other Info	
URL	https://afiliasi.ipwija.ac.id/login
Method	GET
Parameter	XSRF-TOKEN
Attack	
Evidence	set-cookie: XSRF-TOKEN
Other Info	
URL	https://afiliasi.ipwija.ac.id/register
Method	GET
Parameter	XSRF-TOKEN
Attack	
Evidence	set-cookie: XSRF-TOKEN
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	SIAKAD_CLOUD_FRONT_ACCESS
Attack	
Evidence	Set-Cookie: SIAKAD_CLOUD_FRONT_ACCESS
Other Info	
URL	https://afiliasi.ipwija.ac.id/storeRegister
Method	POST
Parameter	XSRF-TOKEN
Attack	
Evidence	set-cookie: XSRF-TOKEN

Other Info	
URL	https://afiliasi.ipwija.ac.id/validateLogin
Method	POST
Parameter	XSRF-TOKEN
Attack	
Evidence	set-cookie: XSRF-TOKEN
Other Info	
Instances	7
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	**Cookie Without Secure Flag**
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	SIAKAD_CLOUD_FRONT_ACCESS
Attack	
Evidence	Set-Cookie: SIAKAD_CLOUD_FRONT_ACCESS
Other Info	
Request Header	GET https://pmb.ipwija.ac.id/ HTTP/1.1 host: pmb.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:10 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Server: Apache **Set-Cookie: SIAKAD_CLOUD_FRONT_ACCESS**=1v8e8gfstl0q5ddfbrb3sojai9; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache SX-Kode-PT: 1519 SX-Role: Peminat SX-User: SX-Session: 1v8e8gfstl0q5ddfbrb3sojai9 SX-Action: view Beranda SX-Action-Result: 1 SX-Message: SX-Referer: https://ipwija.ac.id/ Vary: Accept-Encoding content-length: 36463
Response Body **(truncated)**	<!DOCTYPE html> <html lang="en"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <!-- Load Base CSS --> <link rel="stylesheet" href="https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/css/bootstrap.min.css" /> <!-- Material Icons --> <link href="https://fonts.googleapis.com/css2?family=Material+Icons+Round" rel="stylesheet" /> <link href="ht...(truncated)
Instances	1
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html
CWE Id	614
WASC Id	13
Plugin Id	10011

Low	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://pmb.ipwija.ac.id/

Method	GET
Parameter	SIAKAD_CLOUD_FRONT_ACCESS
Attack	
Evidence	Set-Cookie: SIAKAD_CLOUD_FRONT_ACCESS
Other Info	
Request Header	GET https://pmb.ipwija.ac.id/ HTTP/1.1 host: pmb.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:10 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Server: Apache **Set-Cookie: SIAKAD_CLOUD_FRONT_ACCESS**=1v8e8gfstl0q5ddfbrb3sojai9; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache SX-Kode-PT: 1519 SX-Role: Peminat SX-User: SX-Session: 1v8e8gfstl0q5ddfbrb3sojai9 SX-Action: view Beranda SX-Action-Result: 1 SX-Message: SX-Referer: https://ipwija.ac.id/ Vary: Accept-Encoding content-length: 36463
Response Body **(truncated)**	<!DOCTYPE html> <html lang="en"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <!-- Load Base CSS --> <link rel="stylesheet" href="https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/css/bootstrap.min.css" /> <!-- Material Icons --> <link href="https://fonts.googleapis.com/css2?family=Material+Icons+Round" rel="stylesheet" /> <link href="ht...(truncated)
Instances	1
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
URL	https://afiliasi.ipwija.ac.id/
Method	GET
Parameter	https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
Request Header	GET https://afiliasi.ipwija.ac.id/ HTTP/1.1 host: afiliasi.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:10 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Vary: Accept-Encoding X-Powered-By: PHP/8.2.28 Cache-Control: no-cache, private set-cookie: XSRF-TOKEN=eyJpdiI6IkRWL2pDSXRIVVJLNndZalVobGpkVwc9PSIsInZhbHVlIjoiMjkxV2hQM09NL21YTHZaN2FJLzc3c0VqVzZHSnVxUVMzYmFQVndScnl4Rm1qZGlSUXZtNi9KdnFabjhMbHpNRkFlFlV2VwdmNxd3ZhaWJVaUVPZlZHRiswK3VTenBPZ2NMT3JhSGVzeFY3RTZ2Vy90Z01LSEhBbFFTelU1eHlCTFUiLCJtYWMiOiJlZjM3Mzk1NTBlZjdiNjRjYTlhYzVlMDZmYWZiMzIwNWVjNzY1ZjRiNDJhYmFiMmU3ZWMxZTkzNGElZDc3ZWNjIiwidGFnIjoiI n0%3D; expires=Tue, 18 Nov 2025 03:36:10 GMT; Max-Age=7200; path=/; secure; samesite=lax

set-cookie: laravel_session=eyJpdiI6ImJvVkZqRExGd0hvWXdsZm04bklOVkE9PSIsInZhbHVlIjoiUkpWbmk1aE03TmV1bTg1MTQvMHVGcG0vMUZrRlpMQ2Y3cWx5a29adkpWS0l2VmZDRjdheE9FMHp0NFNKb0F5K0VlWDltOHdnU3FqTGd6Ym9kbDEvRDRiOGVicVdKR2M4ejlCSDAwanloSzVkZ0oyU0lmS2psOXJDQmp4b3F3VTQiLCJtYWMiOiI1NzhkNzQ2MjY3NDNmYWNhNTk0MmJhMjFlMmQ2YjBlYTBmbNWJmOTZlMDk1MzI1ZTQ5NjUxNmRjZTJkYzJiNDQ5IiwidGFn
IjoiIn0%3D; expires=Tue, 18 Nov 2025 03:36:10 GMT; Max-Age=7200; path=/; secure; httponly; samesite=lax
platform: hostinger
panel: hpanel
Content-Security-Policy: upgrade-insecure-requests
Server: hcdn
alt-svc: h3=":443"; ma=86400
x-hcdn-request-id: 4f489f24ae6ec7bc0e1d96f5bc550939-bos-edge4
x-hcdn-cache-status: DYNAMIC
x-hcdn-upstream-rt: 0.825
content-length: 32839

Response Body (excerpt)

```
 <li>Memiliki Email yang aktif dan valid</li>
                        <li>Memiliki Kontak aktif</li>
                    </ol>
                </div>
            </div>
        </div>
    </div>
    <!-- Bootstrap JS and dependencies -->
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js"></script>
    <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
    <script src="https://afiliasi.ipwija.ac.id/assets/js/flickity.pkgd.min.js"></script>

    <script>
        // Komisi Calculator
        $(document).ready(function(
```

URL	https://afiliasi.ipwija.ac.id/
Method	GET
Parameter	https://code.jquery.com/jquery-3.6.0.min.js
Attack	
Evidence	<script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/login
Method	GET
Parameter	//cdn.jsdelivr.net/npm/sweetalert2@11
Attack	
Evidence	<script src="//cdn.jsdelivr.net/npm/sweetalert2@11"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/login
Method	GET
Parameter	https://cdn.datatables.net/1.13.4/js/jquery.dataTables.min.js
Attack	
Evidence	<script src="https://cdn.datatables.net/1.13.4/js/jquery.dataTables.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/login
Method	GET
Parameter	https://cdn.jsdelivr.net/npm/chart.js@3.7.0/dist/chart.min.js
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/chart.js@3.7.0/dist/chart.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/login
Method	GET
Parameter	https://cdn.jsdelivr.net/npm/intro.js/minified/intro.min.js
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/intro.js/minified/intro.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/login
Method	GET
Parameter	https://cdn.jsdelivr.net/npm/select2@4.1.0-rc.0/dist/js/select2.min.js
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/select2@4.1.0-rc.0/dist/js/select2.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/login
Method	GET
Parameter	https://cdn.jsdelivr.net/npm/signature_pad@2.3.2/dist/signature_pad.min.js
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/signature_pad@2.3.2/dist/signature_pad.min.js"></script>
Other Info	

URL	https://afiliasi.ipwija.ac.id/login
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/intro.js/5.0.0/intro.min.js
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/intro.js/5.0.0/intro.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/login
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery.maskedinput/1.4.1/jquery.maskedinput.min.js
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery.maskedinput/1.4.1/jquery.maskedinput.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/login
Method	GET
Parameter	https://code.jquery.com/jquery-3.6.0.min.js
Attack	
Evidence	<script src="https://code.jquery.com/jquery-3.6.0.min.js" crossorigin="anonymous"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/login
Method	GET
Parameter	https://unpkg.com/shepherd.js/dist/js/shepherd.min.js
Attack	
Evidence	<script src="https://unpkg.com/shepherd.js/dist/js/shepherd.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/register
Method	GET
Parameter	//cdn.jsdelivr.net/npm/sweetalert2@11
Attack	
Evidence	<script src="//cdn.jsdelivr.net/npm/sweetalert2@11"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/register
Method	GET
Parameter	https://cdn.datatables.net/1.13.4/js/jquery.dataTables.min.js
Attack	
Evidence	<script src="https://cdn.datatables.net/1.13.4/js/jquery.dataTables.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/register
Method	GET
Parameter	https://cdn.jsdelivr.net/npm/chart.js@3.7.0/dist/chart.min.js
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/chart.js@3.7.0/dist/chart.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/register
Method	GET
Parameter	https://cdn.jsdelivr.net/npm/intro.js/minified/intro.min.js
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/intro.js/minified/intro.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/register
Method	GET
Parameter	https://cdn.jsdelivr.net/npm/select2@4.1.0-rc.0/dist/js/select2.min.js
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/select2@4.1.0-rc.0/dist/js/select2.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/register
Method	GET
Parameter	https://cdn.jsdelivr.net/npm/signature_pad@2.3.2/dist/signature_pad.min.js
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/signature_pad@2.3.2/dist/signature_pad.min.js"></script>
Other Info	

URL	https://afiliasi.ipwija.ac.id/register
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/intro.js/5.0.0/intro.min.js
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/intro.js/5.0.0/intro.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/register
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery.maskedinput/1.4.1/jquery.maskedinput.min.js
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery.maskedinput/1.4.1/jquery.maskedinput.min.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/register
Method	GET
Parameter	https://code.jquery.com/jquery-3.6.0.min.js
Attack	
Evidence	<script src="https://code.jquery.com/jquery-3.6.0.min.js" crossorigin="anonymous"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/register
Method	GET
Parameter	https://unpkg.com/shepherd.js/dist/js/shepherd.min.js
Attack	
Evidence	<script src="https://unpkg.com/shepherd.js/dist/js/shepherd.min.js"></script>
Other Info	
URL	https://ipwija.ac.id/events/ujian-tengah-semester-ganjil/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?onload=wpcaptcha_captcha&render=6Lfus-opAAAAABAkxx5SugKdcFocOz3GjJVJ3y5a&ver=1.30
Attack	
Evidence	<script src='https://www.google.com/recaptcha/api.js?onload=wpcaptcha_captcha&render=6Lfus-opAAAAABAkxx5SugKdcFocOz3GjJVJ3y5a&ver=1.30' id='wpcaptcha-recaptcha-js'></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js
Attack	
Evidence	<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217"></script>
Other Info	

URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js"></script>
Other Info	

URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js
Attack	
Evidence	<script src="https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-91361426-5
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-91361426-5"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js
Attack	
Evidence	<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js"></script>
Other Info	

URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js"></script>
Other Info	

URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js
Attack	
Evidence	<script src="https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-91361426-5
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-91361426-5"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/?lang=id
Method	GET
Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js
Attack	
Evidence	<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js"></script>
Other Info	

URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js"></script>
Other Info	

URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js
Attack	
Evidence	<script src="https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-91361426-5
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-91361426-5"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js"></script>
Other Info	

URL	https://pmb.ipwija.ac.id/home
Method	GET
Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js
Attack	
Evidence	<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916"></script>
Other Info	

URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	GET
Parameter	https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js
Attack	
Evidence	<script src="https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js"></script>
Other Info	

URL		https://pmb.ipwija.ac.id/jalur-seleksi
	Method	GET
	Parameter	https://www.googletagmanager.com/gtag/js?id=UA-91361426-5
	Attack	
	Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-91361426-5"></script>
	Other Info	
URL		https://pmb.ipwija.ac.id/jalur-seleksi
	Method	GET
	Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js
	Attack	
	Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js"></script>
	Other Info	
URL		https://pmb.ipwija.ac.id/jalur-seleksi
	Method	GET
	Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js
	Attack	
	Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js"></script>
	Other Info	
URL		https://pmb.ipwija.ac.id/login
	Method	GET
	Parameter	https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js
	Attack	
	Evidence	<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js"></script>
	Other Info	
URL		https://pmb.ipwija.ac.id/login
	Method	GET
	Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js
	Attack	
	Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js"></script>
	Other Info	
URL		https://pmb.ipwija.ac.id/login
	Method	GET
	Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js
	Attack	
	Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js"></script>
	Other Info	
URL		https://pmb.ipwija.ac.id/login
	Method	GET
	Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729
	Attack	
	Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729"></script>
	Other Info	
URL		https://pmb.ipwija.ac.id/login
	Method	GET
	Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217
	Attack	
	Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217"></script>
	Other Info	
URL		https://pmb.ipwija.ac.id/login
	Method	GET
	Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js
	Attack	
	Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js"></script>
	Other Info	
URL		https://pmb.ipwija.ac.id/login
	Method	GET
	Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js
	Attack	
	Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js"></script>
	Other Info	

URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js"></script>
Other Info	

URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js
Attack	
Evidence	<script src="https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-91361426-5
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-91361426-5"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/login
Method	GET
Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js
Attack	
Evidence	<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217"></script>
Other Info	

URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js"></script>
Other Info	

URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js
Attack	
Evidence	<script src="https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-91361426-5
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-91361426-5"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/pengumuman
Method	GET
Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js
Attack	
Evidence	<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap.min.js"></script>
Other Info	

URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/custom.js?210729"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/forhtml.js?250217"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/id.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-ui-1.10.3.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.ajax.js?210916"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/typeahead.jquery.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.id.js"></script>
Other Info	

URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/js/datepicker.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/background-dim.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js
Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/js/select2.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/bootbox.js/6.0.0/bootbox.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js
Attack	
Evidence	<script src="https://fastly.jsdelivr.net/npm/lightgallery@1.10.0/dist/js/lightgallery-all.min.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-91361426-5
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-91361426-5"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-analytics.js"></script>
Other Info	
URL	https://pmb.ipwija.ac.id/program-studi
Method	GET
Parameter	https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/7.14.1/firebase-app.js"></script>
Other Info	
Instances	177
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Low	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

URL	https://afiliasi.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
Request Header	GET https://afiliasi.ipwija.ac.id/ HTTP/1.1 host: afiliasi.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:10 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Vary: Accept-Encoding **X-Powered-By: PHP/8.2.28** Cache-Control: no-cache, private set-cookie: XSRF-TOKEN=eyJpdiI6IkRWL2pDSXRIVVJLNndZalVobGpkeWc9PSIsInZhbHVlIjoiMjkxV2hQM09NL21YTHZaN2FJLzc3c0VqVzZHSnVxUVMzYmFQVndScnl4Rm1qZGlSUXZtNi9KdnFabjhMbHpNRkFlV2VwdmNxd3ZhaWJVaUVPZlZHRiswK3VTenBPZ2NMT3JhSGVzeFY3RTZ2Vy9OZ01LSEhBbFRTelU1eHlCTFUiLCJtYWMiOiJlZjM3Mzk1NTBlZjdiNjRjRjYTlhYzVlMDZmYWZiMzIwNWVjNzY1ZjRiNDJhYmFiMmU3ZWMxZTkzNGE1ZDc3ZWNjIiwidGFnIjoiIn0%3D; expires=Tue, 18 Nov 2025 03:36:10 GMT; Max-Age=7200; path=/; secure; samesite=lax set-cookie: laravel_session=eyJpdiI6ImJvVkZqRExGd0hvWXdsZm04bklOVkE9PSIsInZhbHVlIjoiUkpWbmk1aE03TmV1bTg1MTQvMHVGcG0vMUZrRlpMQ2Y3cWx5a29adkpWS0l2VmZDRjdheE9FMHp0NFNKb0F5K0VlWDltOHdnU3FqTGd6Ym9kbDEvRDRiOGVicVddKR2M4ejlCSDAwanloSzVkZ0oyU0lmS2psOXJDQmp4b3F3VTQiLCJtYWMiOiI1NzhkNzQ2MjY3NDNNmYWNhNTk0MmJhMjFlMmQ2YjBlYTBmNWJmOTZlMDk1MzI1ZTQ5NjUxNmRjZTJkYzJiNDQ5IiwidGFnIjoiIn0%3D; expires=Tue, 18 Nov 2025 03:36:10 GMT; Max-Age=7200; path=/; secure; httponly; samesite=lax platform: hostinger panel: hpanel Content-Security-Policy: upgrade-insecure-requests Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 4f489f24ae6ec7bc0e1d96f5bc550939-bos-edge4 x-hcdn-cache-status: DYNAMIC x-hcdn-upstream-rt: 0.825 content-length: 32839
Response Body **(truncated)**	<!DOCTYPE html> <html lang="en"> <head> <meta charset="UTF-8"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>Program Afiliasi IPWIJA</title> <!-- Bootstrap CSS --> <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet"> <link rel="preconnect" href="https://fonts.googleapis.com"> <link rel="preconnect" href="https://fonts.gstatic.com" crossorigin> <link href="https://fonts.go...(truncated)
URL	https://ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/?p=20515
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/?p=20523
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/?p=20533
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/?p=20846
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/?p=21009
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/?p=21016
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/?p=21268
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/?p=21354
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/?p=21358
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/?p=21657
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/aktivitas/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/alumni-2/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/arsip/
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/biaya-kuliah-universitas-ipwija/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/buku/hari.%C2%A0%C2%A0
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/comments/feed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/events/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/events/feed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/events/pengisian-krs-genap-2025-2026/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/events/pengumuman-khs-semester-ganjil/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/events/perkuliahan-semester-ganjil-2025-2026/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/events/uji-kompetensi-lsp/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/events/ujian-akhir-semester-ganjil-uas/
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/events/ujian-tengah-semester-ganjil/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/events/wisuda/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/events/yudisium/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/fasilitas/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/feed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/home/u329130267/domains/ipwija.ac.id/public_html/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/hubungi-kami/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/informasi-beasiswa/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/informasi-tes-seleksi/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/kabar-terbaru/
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/kebijakan-dan-pengumuman/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/kemahasiswaan/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/keseharian-di-kampus/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/klinik/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/lembaga-sertifikasi-profesi
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/magister-manajemen/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/marina-goes-to-school-campus-di-universitas-ipwija-no-limit-under-the-sun/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/mengapa-ipwija/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/pendaftaran/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/pengumuman-penerimaan/
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/pentas-seni-universitas-ipwija-2025-youthful-rhapsody-kebebasan-berekspresi/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/perpustakaan/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/program-studi-informatika/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/program-studi-kebidanan/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/program-studi-kewirausahaan/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/program-studi-rekayasa-perangkat-lunak/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/program-studi-sarajana-manajemen/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/program-studi-sistem-informasi/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/pusat-karir/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/pusat-konseling/
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/pusat-teknologi-informasi/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/sekilas-ipwija/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/simulasi-rapor/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/sorotan/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/sosialisasi-p2mw-2025-di-universitas-ipwija-mahasiswa-didorong-jadi-wirausahawan-muda/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/tanggal-penting/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/tentang-universitas-ipwija/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/video/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-content/uploads/2024/10/illustrasi-sarjana-manajemen.jpg
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Faktivitas%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fbiaya-kuliah-universitas-ipwija%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Ffasilitas%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Finformasi-tes-seleksi%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fkeseharian-di-kampus%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fperpustakaan%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fpusat-konseling%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fpusat-teknologi-informasi%2F
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Ftanggal-penting%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Faktivitas%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fbiaya-kuliah-universitas-ipwija%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Ffasilitas%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Finformasi-beasiswa%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Finformasi-tes-seleksi%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fkeseharian-di-kampus%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fperpustakaan%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fpusat-konseling%2F
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fpusat-teknologi-informasi%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fsimulasi-rapor%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Ftanggal-penting%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/wp/v2/pages/15509
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/wp/v2/pages/20515
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/wp/v2/pages/20523
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/wp/v2/pages/20533
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/wp/v2/pages/20846
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/wp/v2/pages/21009
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/wp/v2/pages/21016
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/wp/v2/pages/21268
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/wp/v2/pages/21354
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/wp/v2/pages/21358
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-json/wp/v2/pages/21657
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/wp-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/xmlrpc.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
URL	https://ipwija.ac.id/xmlrpc.php?rsd
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
Instances	102
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10037

Low	Server Leaks Version Information via "Server" HTTP Response Header Field
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	http://repository.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	

Request Header	GET http://repository.ipwija.ac.id/ HTTP/1.1 host: repository.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:10 GMT Server: **Apache/2.4.29 (Ubuntu)** Expires: Thu, 18 Dec 2025 01:36:10 GMT Cache-Control: no-store, no-cache, must-revalidate Vary: Accept-Encoding Content-Type: text/html; charset=utf-8 content-length: 8178
Response Body **(truncated)**	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="X-UA-Compatible" content="IE=edge" /> <title>Welcome to UNIVERSITAS IPWIJA Repository - UNIVERSITAS IPWIJA REPOSITORY</title> <link rel="icon" href="/favicon.ico" type="image/x-icon" /> <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" /> <link rel="alternate" type="...(truncated)
URL	http://repository.ipwija.ac.id/cgi/export/repository/RDFN3/devel.n3
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/cgi/export/repository/RDFXML/devel.rdf
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/cgi/latest
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/cgi/latest_tool?output=Atom
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/cgi/latest_tool?output=RSS
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/cgi/latest_tool?output=RSS2
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/cgi/oai2
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)

Other Info	
URL	http://repository.ipwija.ac.id/cgi/opensearchdescription
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/cgi/register
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/cgi/search
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/cgi/search/advanced
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/cgi/search?_action_search=Search&_order=bytitle&_satisfyall=ALL&basic_srchtype=ALL&q=ZAP
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/cgi/users/home
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/eprints/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/favicon.ico
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/id/contents
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/images/eprintslogo.gif
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)

Other Info	
URL	http://repository.ipwija.ac.id/images/sitelogoipwija.png
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/information.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/javascript/auto-3.3.16.js
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/policies.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/style/auto-3.3.16.css
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/style/ie6.css
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/style/images/feed-icon-14x14.png
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/style/images/message.png
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/sword-app/servicedocument
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)

Other Info	
URL	http://repository.ipwija.ac.id/view/creators/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/creators/index.B.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/creators/index.C.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/creators/index.E.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/creators/index.F-G.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/creators/index.H.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/creators/index.I.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/creators/index.J.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/creators/index.K.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/creators/index.L.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)

Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/fac=5Feng/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/fac=5Flaw/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/fac=5Fmed/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fart/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fecs/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fedu/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fman/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fmat/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fmed/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)

Other Info	
URL	http://repository.ipwija.ac.id/view/divisions/sch=5Fsoc/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/A.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/AC.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/AI.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/AS.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/B.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/BF.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/H.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/H1.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)

Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HB.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HC.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HD.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HD28.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HD61.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HG.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HJ.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HN.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/HV.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/L.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)

Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/LB.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/LB2361.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/Q.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/Q1.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/QA.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/QA75.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/subjects/subjects.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/0031.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/1998.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)

Other Info	
URL	http://repository.ipwija.ac.id/view/year/1999.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2001.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2004.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2005.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2006.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2008.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2009.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2010.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2011.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2012.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)

Other Info	
URL	http://repository.ipwija.ac.id/view/year/2013.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2014.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2015.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2016.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2017.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2018.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2019.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2020.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2021.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2022.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)

Other Info	
URL	http://repository.ipwija.ac.id/view/year/2023.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2024.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/2025.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
URL	http://repository.ipwija.ac.id/view/year/NULL.html
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29 (Ubuntu)
Other Info	
Instances	102
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10036

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://afiliasi.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Request Header	GET https://afiliasi.ipwija.ac.id/ HTTP/1.1 host: afiliasi.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:10 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Vary: Accept-Encoding X-Powered-By: PHP/8.2.28 Cache-Control: no-cache, private set-cookie: XSRF-TOKEN=eyJpdiI6IkRWL2pDSXRIVVJLNndZalVobGpkeWc9PSIsInZhbHVlIjoiMjkxV2hQM09NL21YTHZaN2FJLzc3c0VqVzZHSnVxUVMzYmFQVndScnl4Rm1qZGlSUXZtNi9KdnFabjhMbHpNRkFlV2VwdmNxd3ZhaWJVaUVPZlZHRiswK3VTenBPZ2NMT3JhSGVzeFY3RTZ2Vy9OZ01LSEhBbFRTelU1eHlCTFUiLCJtYWMiOiJlZjM3Mzk1NTBlZjdiNjRjYTlhYzVlMDZmYWZiMzIwNWVjNzY1ZjRiNDJhYmFiMmU3ZWMxZTkzNGE1ZDc3ZWNjIiwidGFnIjoiIn0%3D; expires=Tue, 18 Nov 2025 03:36:10 GMT; Max-Age=7200; path=/; secure; samesite=lax set-cookie: laravel_session=eyJpdiI6ImJvVkZqRExgGd0hvWXdsZm04bklOVkE9PSIsInZhbHVlIjoiUkpWbmk1aE03TmV1bTg1MTQvMHVGcG0vMUZrRlpMQ2Y3cWx5a29adkpwWS0l2VmZDRjdheE9FMHp0NFNKb0F5K0VlWDltOHdnU3FqTGd6Ym9kbDEvRDRiOGVicVdKR2M4ejlCSDAwanloSzVkZ0oyU0lmS2psOXJDQmp4b3F3VTQiLCJtYWMiOiI1NzhkNzQ2MjY3NDNmYWNhNTk0MmJhMjFFMmQ2YjBlYTBmNWJmOTZlMDk1MzI1ZTQ5NjUxNmRjZTJkYzJiNDQ5IiwidGFnIjoiIn0%3D; expires=Tue, 18 Nov 2025 03:36:10 GMT; Max-Age=7200; path=/; secure; httponly; samesite=lax platform: hostinger panel: hpanel Content-Security-Policy: upgrade-insecure-requests Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 4f489f24ae6ec7bc0e1d96f5bc550939-bos-edge4 x-hcdn-cache-status: DYNAMIC

	x-hcdn-upstream-rt: 0.825 content-length: 32839

Response Body **(truncated)**	`<!DOCTYPE html>`
	`<html lang="en">`
	
	`<head>`
	    `<meta charset="UTF-8">`
	    `<meta name="viewport" content="width=device-width, initial-scale=1.0">`
	    `<title>Program Afiliasi IPWIJA</title>`
	    `<!-- Bootstrap CSS -->`
	    `<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">`
	    `<link rel="preconnect" href="https://fonts.googleapis.com">`
	    `<link rel="preconnect" href="https://fonts.gstatic.com" crossorigin>`
	    `<link href="https://fonts.go...(truncated)`

URL	https://ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/%5C%22?page=wsm_traffic&subPage=UsersOnline&subTab=summary%5C%22
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/aktivitas/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/alumni-2/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/arsip/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/biaya-kuliah-universitas-ipwija/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/comments/feed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/fasilitas/
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/feed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/home/u329130267/domains/ipwija.ac.id/public_html/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/hubungi-kami/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/informasi-beasiswa/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/informasi-tes-seleksi/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/kabar-terbaru/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/kebijakan-dan-pengumuman/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/kemahasiswaan/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/keseharian-di-kampus/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/klinik/
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/magister-manajemen/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/marina-goes-to-school-campus-di-universitas-ipwija-no-limit-under-the-sun/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/mengapa-ipwija/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pendaftaran/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pengumuman-penerimaan/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pentas-seni-universitas-ipwija-2025-youthful-rhapsody-kebebasan-berekspresi/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/perpustakaan/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-informatika/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-kebidanan/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-kewirausahaan/
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-rekayasa-perangkat-lunak/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-sarajana-manajemen/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-sistem-informasi/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pusat-karir/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pusat-konseling/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pusat-teknologi-informasi/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/sekilas-ipwija/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/simulasi-rapor/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/sorotan/
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/sosialisasi-p2mw-2025-di-universitas-ipwija-mahasiswa-didorong-jadi-wirausahawan-muda/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/tanggal-penting/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/tentang-universitas-ipwija/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/video/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/chaty/admin/assets/js/picmo-umd.min.js?ver=3.4.1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/chaty/css/chaty-front.min.css?ver=3.4.11742195845
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=6.0.6
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/js/index.js?ver=6.0.6
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/swv/js/index.js?ver=6.0.6
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals/apple-webkit.min.css?ver=3.28.4
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals/e-swiper.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/frontend.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-heading.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-image.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-social-icons.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-spacer.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-video.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/js/frontend-modules.min.js?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/animations/styles/e-animation-pulse.min.css?ver=3.28.4
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/font-awesome/css/all.css?ver=1.3.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/swiper/v8/css/swiper.min.css?ver=8.4.5
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/swiper/v8/swiper.min.js?ver=8.4.5
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/feeds-for-tiktok/vendor/smashballoon/customizer/sb-common/sb-customizer/build/static/css/tikTokFeed.css?ver=6.8.1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/h5p/h5p-php-library/styles/h5p.css?ver=1.16.0
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/insta-gallery/assets/frontend/swiper/swiper.min.css?ver=4.6.1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/insta-gallery/assets/frontend/swiper/swiper.min.js?ver=4.6.1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/insta-gallery/build/frontend/css/style.css?ver=4.6.1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/instagram-feed/css/sbi-styles.min.css?ver=6.9.0
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/interactive-3d-flipbook-powered-physics-engine/assets/js/client-locale-loader.js?ver=1.16.15
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/css/pum-site.min.css?ver=1.20.3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/revslider/public/css/sr7.css?ver=6.7.23
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/revslider/public/js/libs/tptools.js?ver=6.7.23
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/say-what/assets/build/frontend.js?ver=fd31684c45e4d85aeb4e
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/frontend.css?ver=1.3.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/frontend.js?ver=1.3.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/libraries/thim-ekits/css/thim-ekits-icons.min.css?ver=1.3.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/widgets.css?ver=1.3.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/wp-stats-manager/css/style.css?ver=1.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/themes/eduma/assets/css/v4-shims.min.css?ver=5.6.6
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/themes/eduma/assets/js/jquery.waypoints.min.js?ver=5.6.6
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/themes/eduma/style.css?ver=5.6.6
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/uploads/2024/08/cropped-logo-Universitas-1-180x180.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/uploads/2024/08/cropped-logo-Universitas-1-192x192.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-content/uploads/2024/08/cropped-logo-Universitas-1-32x32.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-includes/js/backbone.min.js?ver=1.6.0
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-includes/js/dist/hooks.min.js?ver=4d63a3d491d11ffd8ac6
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-includes/js/dist/i18n.min.js?ver=5e580eb46a90c2b997e6
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-includes/js/imagesloaded.min.js?ver=5.0.0
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-includes/js/jquery/ui/core.min.js?ver=1.13.3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-includes/js/masonry.min.js?ver=4.2.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-includes/js/underscore.min.js?ver=1.13.7
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-includes/js/wp-util.min.js?ver=6.8.1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/wp/v2/pages/15509
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/xmlrpc.php
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/xmlrpc.php?rsd
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	102
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://repository.ipwija.ac.id/
Method	GET
Parameter	x-content-type-options
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.
Request Header	GET http://repository.ipwija.ac.id/ HTTP/1.1 host: repository.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:10 GMT Server: Apache/2.4.29 (Ubuntu) Expires: Thu, 18 Dec 2025 01:36:10 GMT Cache-Control: no-store, no-cache, must-revalidate Vary: Accept-Encoding Content-Type: text/html; charset=utf-8 content-length: 8178
Response Body **(truncated)**	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="X-UA-Compatible" content="IE=edge" /> <title>Welcome to UNIVERSITAS IPWIJA Repository - UNIVERSITAS IPWIJA REPOSITORY</title> <link rel="icon" href="/favicon.ico" type="image/x-icon" /> <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" /> <link rel="alternate" type="...(truncated)
URL	https://afiliasi.ipwija.ac.id/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/

Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/aktivitas/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/alumni-2/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/arsip/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/biaya-kuliah-universitas-ipwija/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/comments/feed/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/events/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/fasilitas/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/feed/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/hubungi-kami/
Method	GET

Parameter	x-content-type-options
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://ipwija.ac.id/informasi-beasiswa/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/informasi-tes-seleksi/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/kabar-terbaru/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/kebijakan-dan-pengumuman/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/kemahasiswaan/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/keseharian-di-kampus/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/klinik/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/magister-manajemen/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/marina-goes-to-school-campus-di-universitas-ipwija-no-limit-under-the-sun/
Method	GET
Parameter	x-content-type-options

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://ipwija.ac.id/mengapa-ipwija/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/pendaftaran/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/pengumuman-penerimaan/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/pentas-seni-universitas-ipwija-2025-youthful-rhapsody-kebebasan-berekspresi/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/perpustakaan/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/program-studi-informatika/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/program-studi-kebidanan/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/program-studi-kewirausahaan/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/program-studi-rekayasa-perangkat-lunak/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/program-studi-sarajana-manajemen/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/program-studi-sistem-informasi/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/pusat-karir/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/pusat-konseling/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/pusat-teknologi-informasi/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/robots.txt
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/sekilas-ipwija/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/simulasi-rapor/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/sorotan/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/sosialisasi-p2mw-2025-di-universitas-ipwija-mahasiswa-didorong-jadi-wirausahawan-muda/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/tanggal-penting/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/tentang-universitas-ipwija/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/video/
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/chaty/admin/assets/js/picmo-latest-umd.min.js?ver=3.4.1
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/chaty/admin/assets/js/picmo-umd.min.js?ver=3.4.1
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/chaty/css/chaty-front.min.css?ver=3.4.11742195845
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=6.0.6
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/js/index.js?ver=6.0.6
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/swv/js/index.js?ver=6.0.6
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals/apple-webkit.min.css?ver=3.28.4
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals/e-swiper.min.css?ver=3.28.4
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/css/frontend.min.css?ver=3.28.4
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-heading.min.css?ver=3.28.4
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-image.min.css?ver=3.28.4
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-social-icons.min.css?ver=3.28.4
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-spacer.min.css?ver=3.28.4
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-video.min.css?ver=3.28.4
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/js/frontend-modules.min.js?ver=3.28.4

Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.28.4
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/animations/styles/e-animation-pulse.min.css?ver=3.28.4
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/font-awesome/css/all.css?ver=1.3.2
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/swiper/v8/css/swiper.min.css?ver=8.4.5
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/swiper/v8/swiper.min.js?ver=8.4.5
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/feeds-for-tiktok/vendor/smashballoon/customizer/sb-common/sb-customizer/build/static/css/tikTokFeed.css?ver=6.8.1
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/h5p/h5p-php-library/styles/h5p.css?ver=1.16.0
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/insta-gallery/assets/frontend/swiper/swiper.min.css?ver=4.6.1
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/insta-gallery/assets/frontend/swiper/swiper.min.js?ver=4.6.1
Method	GET

Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/insta-gallery/build/frontend/css/style.css?ver=4.6.1
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/instagram-feed/css/sbi-styles.min.css?ver=6.9.0
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/instagram-feed/js/sbi-scripts.min.js?ver=6.9.0
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/interactive-3d-flipbook-powered-physics-engine/assets/js/client-locale-loader.js?ver=1.16.15
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/popup-maker/assets/css/pum-site.min.css?ver=1.20.3
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/popup-maker/assets/js/vendor/mobile-detect.min.js?ver=1.3.3
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/revslider/public/css/sr7.css?ver=6.7.23
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/revslider/public/js/libs/tptools.js?ver=6.7.23
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/revslider/public/js/sr7.js?ver=6.7.23
Method	GET
Parameter	x-content-type-options

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://ipwija.ac.id/wp-content/plugins/say-what/assets/build/frontend.js?ver=fd31684c45e4d85aeb4e
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/frontend.css?ver=1.3.2
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/frontend.js?ver=1.3.2
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/libraries/thim-ekits/css/thim-ekits-icons.min.css?ver=1.3.2
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/widgets.css?ver=1.3.2
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/plugins/wp-stats-manager/css/style.css?ver=1.2
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/themes/eduma/assets/css/v4-shims.min.css?ver=5.6.6
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/themes/eduma/assets/js/jquery.countTo.min.js?ver=5.6.6
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/themes/eduma/assets/js/jquery.waypoints.min.js?ver=5.6.6
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/themes/eduma/style.css?ver=5.6.6
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/uploads/2024/08/cropped-logo-Universitas-1-180x180.png
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/uploads/2024/08/cropped-logo-Universitas-1-192x192.png
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-content/uploads/2024/08/cropped-logo-Universitas-1-32x32.png
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-includes/js/backbone.min.js?ver=1.6.0
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-includes/js/dist/api-fetch.min.js?ver=3623a576c78df404ff20
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-includes/js/dist/hooks.min.js?ver=4d63a3d491d11ffd8ac6
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-includes/js/dist/i18n.min.js?ver=5e580eb46a90c2b997e6
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-includes/js/imagesloaded.min.js?ver=5.0.0
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-includes/js/jquery/ui/core.min.js?ver=1.13.3
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-includes/js/masonry.min.js?ver=4.2.2
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-includes/js/underscore.min.js?ver=1.13.7
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/wp-includes/js/wp-util.min.js?ver=6.8.1
Method	GET
Parameter	x-content-type-options
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://ipwija.ac.id/xmlrpc.php?rsd
Method	GET
Parameter	x-content-type-options
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://pmb.ipwija.ac.id/
Method	GET
Parameter	x-content-type-options
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	102
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	Authentication Request Identified
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	https://afiliasi.ipwija.ac.id/validateLogin
Method	POST
Parameter	email
Attack	
Evidence	password
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=password referer=https://afiliasi.ipwija.ac.id/login csrfToken=_token
Request Header	POST https://afiliasi.ipwija.ac.id/validateLogin HTTP/1.1 host: afiliasi.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache content-type: application/x-www-form-urlencoded referer: https://afiliasi.ipwija.ac.id/login content-length: 88 Cookie: XSRF-TOKEN=eyJpdiI6IktuVjdmQ2syRHlRQlRRd3VYbWgvcXc9PSIsInZhbHVlIjoiTWoxQWZWTUhLVzMyalhaamxnY0tRK25oM0hVZThvbjZlY2JxdHdBbkpud1lNcC9kMXZX0TZoMDVGUHYxRnhEdlVBL0hkbUpITDNUc1J2MmpMbWlQN3Zxd0hjc2pEYjVvdmZ6b3g4b2duR2o0UE8wR3NUZDhwa2hYd1hiR2JnVXUiLCJtYWMiOiJlZTZjM2NlYjM2ZDYwN2FkNTk2ZjA5YzdkMTdlNjI1YWExZjE2M2YyYTE5ZDFkNDMyMTQ3YTg0MTViYjY0YzVkIiwidGFnIjoiIn0%3D; laravel_session=eyJpdiI6InVweVA1M01Lc0hhcmV5WE40Sk1IbFE9PSIsInZhbHVlIjoiUFBSWG96U2EzbmxvQ01YU0t6dEdKSGVYUnYzYW9mWTJyRGpjNG9tWDNsTndxUWo5bFZRa3dST1E4cEpEdERy0DQ5R1RHM3RWMHQvSjlLNjN0ZW5hV054TVhVUmJHZkI2OFZuU3hVc0lyajJscCXhxT2diNTljK3pCT3RtejBYTUkiLCJtYWMiOiIzNjBkYmQ4ZThiNjM1ZTAzNDM5NTlhZjdjjMDM0MTdiNWM1OTEyNDVjNzM4MjUyODk4MWJkMGJmMTU4NjRmY2I0IiwidGFnIjoiIn0%3D
Request Body	_token=R2krtMMVY333iJMlv6DpUCm9nqE1KK26GRt1fXv0&email=zaproxy%40example.com&password=ZAP
Response Header	HTTP/1.1 302 Found Date: Tue, 18 Nov 2025 01:38:48 GMT Content-Type: text/html; charset=utf-8 Connection: keep-alive Vary: Accept-Encoding X-Powered-By: PHP/8.2.28 Cache-Control: no-cache, no-store, must-revalidate, max-age=0 Location: https://afiliasi.ipwija.ac.id/login set-cookie: XSRF-TOKEN=eyJpdiI6ImhKY2lrV0R2cS9PUXNHK3JFaW85S1E9PSIsInZhbHVlIjoiZm5qdE5ja0FNeWNGUXR3S2d2TmdKQm5MQ0tDcGJvVFYwcTViWXJxZE1SR2M4QUhnaHF2eW42TVVBT1lyS2c5aTVpWmlIMmdjTTYzcmhrZzJNRmVxSVZnaGZlcmozbDRUWlZFdFIrREtPVU9xSFVwb1ZyRXhHR0tWaUphdkZCVmYiLCJtYWMiOiI4Nzg0MGE2ZTRl0WJjNWUwODgzODRiMzI2Y2QxYWNmYTIwZjlhZDkz0DUyOGYz0WNmZGFkMDli0DY4YzYzYTk1IiwidGFnIjoiIn0%3D; expires=Tue, 18 Nov 2025 03:38:48 GMT; Max-Age=7200; path=/; secure; samesite=lax set-cookie: laravel_session=eyJpdiI6Ik5VYTdJOEpIbXJHcmRkdHFRTnk2QlE9PSIsInZhbHVlIjoiT2pjMCtMK0dxTy9ubEJidS9lRHd3b3lkWE1kRjhVc2FSMUhMdWV1UFY1MXdBRi8rcjNSUnZnY29ERklib3BpK3RvQnFFYWl1azdzc2JodnJTU0laOStwOGNpNlFHNnlLS3dJTVhtVnpVWDkvWUJXaUZVWkdmdDU1N0tTMTFRY0kiLCJtYWMiOiIzMzIwMDRhM2UxNmI4MGM1N2M5YzU3ZWU5MzEyMzNiZWIzYmJmZWM5NDExM2IwMjdiZGNiMGI5ZmEwMTBiNDMzIiwidGFnIjoiIn0%3D; expires=Tue, 18 Nov 2025 03:38:48 GMT; Max-Age=7200; path=/; secure; httponly; samesite=lax platform: hostinger panel: hpanel Content-Security-Policy: upgrade-insecure-requests Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 333d62dd58da664496a9ba49db5f7382-bos-edge4 x-hcdn-cache-status: DYNAMIC x-hcdn-upstream-rt: 0.799 content-length: 386

Response Body	`<!DOCTYPE html>`
	`<html>`
	`    <head>`
	`        <meta charset="UTF-8" />`
	`        <meta http-equiv="refresh" content="0;url='https://afiliasi.ipwija.ac.id/login'" />`
	
	`        <title>Redirecting to https://afiliasi.ipwija.ac.id/login</title>`
	`    </head>`
	`    <body>`
	`        Redirecting to <a href="https://afiliasi.ipwija.ac.id/login">https://afiliasi.ipwija.ac.id/login</a>.`
	`    </body>`
	`</html>`

Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	Charset Mismatch
Description	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set. An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2F
Method	GET
Parameter	
Attack	

Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
Request Header	GET https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2F HTTP/1.1 host: ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:12 GMT Content-Type: text/xml; charset=UTF-8 Connection: keep-alive Vary: Accept-Encoding X-Powered-By: PHP/8.2.28 X-Robots-Tag: noindex Link: <https://ipwija.ac.id/wp-json/>; rel="https://api.w.org/" X-Content-Type-Options: nosniff Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link Access-Control-Allow-Headers: Authorization, X-WP-Nonce, Content-Disposition, Content-MD5, Content-Type Allow: GET Etag: W/"2814-1763429665;gz" X-LiteSpeed-Cache: hit platform: hostinger panel: hpanel Content-Security-Policy: upgrade-insecure-requests Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: f3bf308f2f12650e5cd3e1cfa578a886-bos-edge5 x-hcdn-cache-status: MISS x-hcdn-upstream-rt: 0.752 content-length: 2267
Response Body **(truncated)**	<?xml version="1.0"?> <oembed><version>1.0</version><provider_name>Universitas IPWIJA</provider_name><provider_url>https://ipwija.ac.id</provider_url><author_name>Humas IPWIJA</author_name><author_url>https://ipwija.ac.id/author/uipwija/</author_url><title>University</title><type>rich</type><width>600</width><height>338</height><html><blockquote class="wp-embedded-content" data-secret="kCilaRnNQa">University</blockquote><iframe sandb...(truncated)
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Faktivitas%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Falumni-2%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Farsip%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fbiaya-kuliah-universitas-ipwija%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fevents%2Fpengisian-krs-genap-2025-2026%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fevents%2Fpengumuman-khs-semester-ganjil%2F
Method	GET
Parameter	

Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fevents%2Fperkuliahan-semester-ganjil-2025-2026%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fevents%2Fuji-kompetensi-lsp%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fevents%2Fujian-akhir-semester-ganjil-uas%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fevents%2Fujian-tengah-semester-ganjil%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fevents%2Fwisuda%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fevents%2Fyudisium%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Ffasilitas%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fhubungi-kami%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Finformasi-beasiswa%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Finformasi-tes-seleksi%2F
Method	GET
Parameter	

Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fkabar-terbaru%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fkebijakan-dan-pengumuman%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fkemahasiswaan%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fkeseharian-di-kampus%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fklinik%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fmagister-manajemen%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fmarina-goes-to-school-campus-di-universitas-ipwija-no-limit-under-the-sun%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fmengapa-ipwija%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fpendaftaran%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fpengumuman-penerimaan%2F
Method	GET
Parameter	

Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fperpustakaan%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-informatika%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-kebidanan%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-kewirausahaan%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-rekayasa-perangkat-lunak%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-sarajana-manajemen%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-sistem-informasi%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fpusat-karir%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fpusat-konseling%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fpusat-teknologi-informasi%2F
Method	GET
Parameter	

Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fsekilas-ipwija%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fsimulasi-rapor%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fsorotan%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fsosialisasi-p2mw-2025-di-universitas-ipwija-mahasiswa-didorong-jadi-wirausahawan-muda%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Ftanggal-penting%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Ftentang-universitas-ipwija%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fvideo%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
Instances	44
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011

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://afiliasi.ipwija.ac.id/
Method	GET
Parameter	cache-control
Attack	
Evidence	no-cache, private
Other Info	

| Request Header | ```
GET https://afiliasi.ipwija.ac.id/ HTTP/1.1
host: afiliasi.ipwija.ac.id
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: https://ipwija.ac.id/
``` |
| Request Body | |
| Response Header | ```
HTTP/1.1 200 OK
Date: Tue, 18 Nov 2025 01:36:10 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/8.2.28
Cache-Control: no-cache, private
set-cookie: XSRF-TOKEN=eyJpdiI6IkRWL2pDSXRIVVJLNndZalVobGpkeWc9PSIsInZhbHVlIjoiMjkxV2hQM09NL21YTHZaN2FJLzc3c0VqVzZHSnVxUVMzYmFQVndScnl4Rm1qZGlSUXZtNi9KdnFabjhMbHpNRkFlV2VwdmNxd3ZhaWJVaUVPZlZHRiswK3VTenBPZ2NMT3JhSGVzeFY3RTZ2Vy9OZ01LSEhBbFRTelU1eHlCTFUiLCJtYWMiOiJlZjM3Mzk1NTBlZjdiNjRjYTlhYzVlMDZmYWZiMzIwNWVjNzYlZjRiNDJhYmFiMmU3ZWMxZTkzNGE1ZDc3ZWNjIiwidGFnIjoiIn0%3D; expires=Tue, 18 Nov 2025 03:36:10 GMT; Max-Age=7200; path=/; secure; samesite=lax
set-cookie: laravel_session=eyJpdiI6ImJvVkZqRExGd0hvWXdsZm04bklOVkE9PSIsInZhbHVlIjoiUkpWbmk1aE03TmV1bTg1MTQvMHVGcG0vMUZrRlpMQ2Y3cWx5a29adkpWS0l2VmZDRjdheE9FMHp0NFNKb0F5K0VlWDltOHdnU3FqTGd6Ym9kbEvRDRiOGVicVdkKR2M4ejlCSDAwanloSzVkZ0oyU0lmS2psOXJDQmp4b3F3VTQiLCJtYWMiOiI1NzhkNzQ2MjY3NDNmYWNhNTk0MmJhMjFlMmQ2YjBlYTBmNWJmOTZlMDk1MzI1ZTQ5NjUxNmRjZTJkYzJiNDQ5IiwidGFnIjoiIn0%3D; expires=Tue, 18 Nov 2025 03:36:10 GMT; Max-Age=7200; path=/; secure; httponly; samesite=lax
platform: hostinger
panel: hpanel
Content-Security-Policy: upgrade-insecure-requests
Server: hcdn
alt-svc: h3=":443"; ma=86400
x-hcdn-request-id: 4f489f24ae6ec7bc0e1d96f5bc550939-bos-edge4
x-hcdn-cache-status: DYNAMIC
x-hcdn-upstream-rt: 0.825
content-length: 32839
``` |
| Response Body **(truncated)** | ```
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Program Afiliasi IPWIJA</title>
    <!-- Bootstrap CSS -->
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
    <link rel="preconnect" href="https://fonts.googleapis.com">
    <link rel="preconnect" href="https://fonts.gstatic.com" crossorigin>
    <link href="https://fonts.go...(truncated)
``` |
URL	https://ipwija.ac.id/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/aktivitas/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/alumni-2/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/arsip/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/banjir-di-bekasi-civitas-ipwija-gotong-royong-pulihkan-lingkungan/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/bem-universitas-ipwija-sukses-gelar-iscom-2025-ajang-kompetisi-olahraga-penuh-semangat/

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/biaya-kuliah-universitas-ipwija/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/category/kegiatan-mahasiswa/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/comments/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/pengisian-krs-genap-2025-2026/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/pengumuman-khs-semester-ganjil/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/perkuliahan-semester-ganjil-2025-2026/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/uji-kompetensi-lsp/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/ujian-akhir-semester-ganjil-uas/

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/ujian-tengah-semester-ganjil/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/wisuda/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/events/yudisium/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/fasilitas/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/hubungi-kami/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/informasi-beasiswa/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/informasi-tes-seleksi/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/kabar-terbaru/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/kebijakan-dan-pengumuman/

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/kemahasiswaan/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/keseharian-di-kampus/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/klinik/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/magister-manajemen/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/marina-goes-to-school-campus-di-universitas-ipwija-no-limit-under-the-sun/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/mengapa-ipwija/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pendaftaran/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pengumuman-penerimaan/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pentas-seni-universitas-ipwija-2025-youthful-rhapsody-kebebasan-berekspresi/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/perpustakaan/

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-informatika/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-kebidanan/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-kewirausahaan/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-rekayasa-perangkat-lunak/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-sarajana-manajemen/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/program-studi-sistem-informasi/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pusat-karir/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pusat-konseling/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/pusat-teknologi-informasi/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/robots.txt

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/sekilas-ipwija/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/silaturahmi-pascalebaran-universitas-ipwija-gelar-halal-bihalal-bersama-pimpinan-yayasan-dan-universitas/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/simulasi-rapor/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/sorotan/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/sosialisasi-p2mw-2025-di-universitas-ipwija-mahasiswa-didorong-jadi-wirausahawan-muda/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/tanggal-penting-pendaftaran/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/tanggal-penting/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/tentang-universitas-ipwija/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/video/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Faktivitas%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fbiaya-kuliah-universitas-ipwija%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Ffasilitas%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Finformasi-beasiswa%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Finformasi-tes-seleksi%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fkemahasiswaan%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fkeseharian-di-kampus%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fklinik%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fmagister-manajemen%2F

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fpendaftaran%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fpengumuman-penerimaan%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fperpustakaan%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-informatika%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-kewirausahaan%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-rekayasa-perangkat-lunak%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-sistem-informasi%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fpusat-konseling%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fpusat-teknologi-informasi%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Fsimulasi-rapor%2F

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Ftanggal-penting%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fipwija.ac.id%2Ftentang-universitas-ipwija%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Faktivitas%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fbiaya-kuliah-universitas-ipwija%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Ffasilitas%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Finformasi-beasiswa%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Finformasi-tes-seleksi%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fkemahasiswaan%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fkeseharian-di-kampus%2F

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fklinik%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fmagister-manajemen%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fpendaftaran%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fpengumuman-penerimaan%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fperpustakaan%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-informatika%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-kewirausahaan%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-rekayasa-perangkat-lunak%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fprogram-studi-sistem-informasi%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fpusat-konseling%2F

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fpusat-teknologi-informasi%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fsimulasi-rapor%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Ftanggal-penting%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Ftentang-universitas-ipwija%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://ipwija.ac.id/wp-sitemap.xml
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
Instances	102
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

Informational	Retrieved from Cache
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	Age: 526
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Request Header	GET https://ipwija.ac.id/ HTTP/1.1 host: ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:07 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive

```
Vary: Accept-Encoding
X-Powered-By: PHP/8.2.28
Link: <https://ipwija.ac.id/wp-json/>; rel="https://api.w.org/"
Link: <https://ipwija.ac.id/wp-json/wp/v2/pages/15509>; rel="alternate"; title="JSON"; type="application/json"
Link: <https://ipwija.ac.id/>; rel=shortlink
Etag: W/"99-1762975106;gz"
X-LiteSpeed-Cache: hit
platform: hostinger
panel: hpanel
Content-Security-Policy: upgrade-insecure-requests
Age: 526
Server: hcdn
alt-svc: h3=":443"; ma=86400
x-hcdn-request-id: 1c7fc13d5ff49deccd08f5a201f8b8f8-bos-edge4
x-hcdn-cache-status: HIT
content-length: 415329
```

Response Body **(truncated)**	`<!DOCTYPE html>`
	`<html itemscope itemtype="http://schema.org/WebPage" lang="en-US">`
	`<head>`
	`        <meta charset="UTF-8">`
	`        <meta name="viewport" content="width=device-width, initial-scale=1">`
	`        <link rel="profile" href="http://gmpg.org/xfn/11">`
	`        <link rel="pingback" href="https://ipwija.ac.id/xmlrpc.php">`
	`        <title>Universitas IPWIJA – Universitas IPWIJA</title>`
	`<style>`
	`#wpadminbar #wp-admin-bar-wsm_free_top_button .ab-icon:before {`
	`        content: "\f239";`
	`        color: #FF9800;`
	`        top: 3px;`
	`}`
	`</style><meta name=...(truncated)`

URL	https://ipwija.ac.id/aktivitas/
Method	GET
Parameter	
Attack	
Evidence	Age: 56601
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/arsip/
Method	GET
Parameter	
Attack	
Evidence	Age: 107
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/biaya-kuliah-universitas-ipwija/
Method	GET
Parameter	
Attack	
Evidence	Age: 66453
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/events/
Method	GET
Parameter	
Attack	
Evidence	Age: 60
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/events/wisuda/
Method	GET
Parameter	
Attack	
Evidence	Age: 91
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/fasilitas/
Method	GET
Parameter	
Attack	
Evidence	Age: 28075
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/hubungi-kami/
Method	GET
Parameter	
Attack	

Evidence	Age: 57
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/informasi-tes-seleksi/
Method	GET
Parameter	
Attack	
Evidence	Age: 60
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/kabar-terbaru/
Method	GET
Parameter	
Attack	
Evidence	Age: 108
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/kebijakan-dan-pengumuman/
Method	GET
Parameter	
Attack	
Evidence	Age: 58
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/kemahasiswaan/
Method	GET
Parameter	
Attack	
Evidence	Age: 109
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/keseharian-di-kampus/
Method	GET
Parameter	
Attack	
Evidence	Age: 109
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/klinik/
Method	GET
Parameter	
Attack	
Evidence	Age: 60
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/magister-manajemen/
Method	GET
Parameter	
Attack	
Evidence	Age: 60
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/marina-goes-to-school-campus-di-universitas-ipwija-no-limit-under-the-sun/
Method	GET
Parameter	
Attack	
Evidence	Age: 58
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/perpustakaan/
Method	GET
Parameter	
Attack	
Evidence	Age: 59
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/program-studi-informatika/
Method	GET
Parameter	
Attack	

Evidence	Age: 68513
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/program-studi-kewirausahaan/
Method	GET
Parameter	
Attack	
Evidence	Age: 60139
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/program-studi-rekayasa-perangkat-lunak/
Method	GET
Parameter	
Attack	
Evidence	Age: 51275
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/program-studi-sistem-informasi/
Method	GET
Parameter	
Attack	
Evidence	Age: 21556
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/pusat-konseling/
Method	GET
Parameter	
Attack	
Evidence	Age: 108
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/pusat-teknologi-informasi/
Method	GET
Parameter	
Attack	
Evidence	Age: 108
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/robots.txt
Method	GET
Parameter	
Attack	
Evidence	Age: 109
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/sosialisasi-p2mw-2025-di-universitas-ipwija-mahasiswa-didorong-jadi-wirausahawan-muda/
Method	GET
Parameter	
Attack	
Evidence	Age: 58
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/tanggal-penting/
Method	GET
Parameter	
Attack	
Evidence	Age: 109
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/chaty/admin/assets/js/picmo-umd.min.js?ver=3.4.1
Method	GET
Parameter	
Attack	
Evidence	Age: 57
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=6.0.6
Method	GET
Parameter	
Attack	

Evidence	Age: 108
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/js/index.js?ver=6.0.6
Method	GET
Parameter	
Attack	
Evidence	Age: 57
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals/apple-webkit.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	Age: 106
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals/e-swiper.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	Age: 107
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/frontend.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	Age: 58
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-heading.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	Age: 58
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-image.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	Age: 58
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-social-icons.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	Age: 106
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-spacer.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	Age: 58
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/js/frontend-modules.min.js?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	Age: 56
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.28.4
Method	GET
Parameter	
Attack	

Evidence	Age: 56
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/animations/styles/e-animation-pulse.min.css?ver=3.28.4
Method	GET
Parameter	
Attack	
Evidence	Age: 107
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/font-awesome/css/all.css?ver=1.3.2
Method	GET
Parameter	
Attack	
Evidence	Age: 57
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/swiper/v8/css/swiper.min.css?ver=8.4.5
Method	GET
Parameter	
Attack	
Evidence	Age: 107
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/swiper/v8/swiper.min.js?ver=8.4.5
Method	GET
Parameter	
Attack	
Evidence	Age: 105
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/feeds-for-tiktok/vendor/smashballoon/customizer/sb-common/sb-customizer/build/static/css/tikTokFeed.css?ver=6.8.1
Method	GET
Parameter	
Attack	
Evidence	Age: 58
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/h5p/h5p-php-library/styles/h5p.css?ver=1.16.0
Method	GET
Parameter	
Attack	
Evidence	Age: 58
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/insta-gallery/build/frontend/css/style.css?ver=4.6.1
Method	GET
Parameter	
Attack	
Evidence	Age: 58
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/interactive-3d-flipbook-powered-physics-engine/assets/js/client-locale-loader.js?ver=1.16.15
Method	GET
Parameter	
Attack	
Evidence	Age: 106
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/css/pum-site.min.css?ver=1.20.3
Method	GET
Parameter	
Attack	
Evidence	Age: 58
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/say-what/assets/build/frontend.js?ver=fd31684c45e4d85aeb4e
Method	GET
Parameter	
Attack	

Evidence	Age: 57
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/libraries/thim-ekits/css/thim-ekits-icons.min.css?ver=1.3.2
Method	GET
Parameter	
Attack	
Evidence	Age: 106
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/plugins/wp-stats-manager/css/style.css?ver=1.2
Method	GET
Parameter	
Attack	
Evidence	Age: 107
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/themes/eduma/assets/js/jquery.waypoints.min.js?ver=5.6.6
Method	GET
Parameter	
Attack	
Evidence	Age: 105
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/08/cropped-logo-Universitas-1-180x180.png
Method	GET
Parameter	
Attack	
Evidence	Age: 105
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/08/cropped-logo-Universitas-1-192x192.png
Method	GET
Parameter	
Attack	
Evidence	Age: 106
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/im-2-100x100.png
Method	GET
Parameter	
Attack	
Evidence	Age: 104
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/im-3-150x150.png
Method	GET
Parameter	
Attack	
Evidence	Age: 104
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/im-3-300x300.png
Method	GET
Parameter	
Attack	
Evidence	Age: 55
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-1-300x160.png
Method	GET
Parameter	
Attack	
Evidence	Age: 55
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-10-1024x545.png
Method	GET
Parameter	
Attack	

Evidence	Age: 56
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-10-600x320.png
Method	GET
Parameter	
Attack	
Evidence	Age: 103
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-10.png
Method	GET
Parameter	
Attack	
Evidence	Age: 102
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-11-1536x818.png
Method	GET
Parameter	
Attack	
Evidence	Age: 103
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-11.png
Method	GET
Parameter	
Attack	
Evidence	Age: 55
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-13-1536x818.png
Method	GET
Parameter	
Attack	
Evidence	Age: 102
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-13.png
Method	GET
Parameter	
Attack	
Evidence	Age: 55
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-14-300x160.png
Method	GET
Parameter	
Attack	
Evidence	Age: 104
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-14-600x320.png
Method	GET
Parameter	
Attack	
Evidence	Age: 56
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-16-600x320.png
Method	GET
Parameter	
Attack	
Evidence	Age: 55
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-16.png
Method	GET
Parameter	
Attack	

Evidence	Age: 54
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-17-1536x818.png
Method	GET
Parameter	
Attack	
Evidence	Age: 53
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-17-300x160.png
Method	GET
Parameter	
Attack	
Evidence	Age: 54
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-17-768x409.png
Method	GET
Parameter	
Attack	
Evidence	Age: 100
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-17.png
Method	GET
Parameter	
Attack	
Evidence	Age: 99
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-18-300x160.png
Method	GET
Parameter	
Attack	
Evidence	Age: 100
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-2-1536x818.png
Method	GET
Parameter	
Attack	
Evidence	Age: 54
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-2.png
Method	GET
Parameter	
Attack	
Evidence	Age: 54
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-20-600x320.png
Method	GET
Parameter	
Attack	
Evidence	Age: 100
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-21-1024x545.png
Method	GET
Parameter	
Attack	
Evidence	Age: 100
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-21-768x409.png
Method	GET
Parameter	
Attack	

Evidence	Age: 55
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-3-1024x545.png
Method	GET
Parameter	
Attack	
Evidence	Age: 54
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-3-1536x818.png
Method	GET
Parameter	
Attack	
Evidence	Age: 101
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-3-300x160.png
Method	GET
Parameter	
Attack	
Evidence	Age: 102
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-3-768x409.png
Method	GET
Parameter	
Attack	
Evidence	Age: 101
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-3.png
Method	GET
Parameter	
Attack	
Evidence	Age: 54
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-4-600x320.png
Method	GET
Parameter	
Attack	
Evidence	Age: 55
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-5-600x321.png
Method	GET
Parameter	
Attack	
Evidence	Age: 101
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-5.png
Method	GET
Parameter	
Attack	
Evidence	Age: 101
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-6-1024x545.png
Method	GET
Parameter	
Attack	
Evidence	Age: 101
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-6.png
Method	GET
Parameter	
Attack	

Evidence	Age: 101
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-7-300x160.png
Method	GET
Parameter	
Attack	
Evidence	Age: 55
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-7-600x320.png
Method	GET
Parameter	
Attack	
Evidence	Age: 101
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-8.png
Method	GET
Parameter	
Attack	
Evidence	Age: 56
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2024/09/Logo-9.png
Method	GET
Parameter	
Attack	
Evidence	Age: 103
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2025/05/Edit-Shandy-FEB.png
Method	GET
Parameter	
Attack	
Evidence	Age: 55
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/2025/05/Edit-Shandy-FSK-2.png
Method	GET
Parameter	
Attack	
Evidence	Age: 102
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-content/uploads/sb-instagram-feed-images/universitasipwija.webp
Method	GET
Parameter	
Attack	
Evidence	Age: 56
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-includes/js/backbone.min.js?ver=1.6.0
Method	GET
Parameter	
Attack	
Evidence	Age: 57
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-includes/js/dist/api-fetch.min.js?ver=3623a576c78df404ff20
Method	GET
Parameter	
Attack	
Evidence	Age: 105
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-includes/js/dist/i18n.min.js?ver=5e580eb46a90c2b997e6
Method	GET
Parameter	
Attack	

Evidence	Age: 105
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-includes/js/imagesloaded.min.js?ver=5.0.0
Method	GET
Parameter	
Attack	
Evidence	Age: 105
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
Method	GET
Parameter	
Attack	
Evidence	Age: 106
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-includes/js/underscore.min.js?ver=1.13.7
Method	GET
Parameter	
Attack	
Evidence	Age: 105
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://ipwija.ac.id/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fipwija.ac.id%2Fbiaya-kuliah-universitas-ipwija%2F
Method	GET
Parameter	
Attack	
Evidence	Age: 37
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	102
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	525
WASC Id	
Plugin Id	10050

Informational	Session Management Response Identified
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	https://afiliasi.ipwija.ac.id/
Method	GET
Parameter	laravel_session
Attack	
Evidence	laravel_session
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
Request Header	GET https://afiliasi.ipwija.ac.id/ HTTP/1.1 host: afiliasi.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://ipwija.ac.id/
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:36:10 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Vary: Accept-Encoding X-Powered-By: PHP/8.2.28 Cache-Control: no-cache, private set-cookie: XSRF-TOKEN=eyJpdiI6IkRWL2pDSXRIVVJLNndZalVobGpkeWc9PSIsInZhbHVlIjoiMjkxV2hQM09NL21YTHZaN2FJLzc3c0VqVzZHSnVxUVMzYmFQVndScnl4Rm1qZGlSUXZtNi9KdnFabjhMbHpNRkFlV2VwdmNxd3ZhaWJVaUVPZlZHRiswK3VTenBPZ2NMT3JhSGVzeFY3RTZ2Vy9OZ20lLSEhBbFRTelU1eEHlCTFUiLCJtYWMiOiJlZjM3Mzk1NTBlZjdiNjRjYTlhYzVlMDZmYWZiMzIwNWVjNzYlZjRiNDJhYmFiMmU3ZWMxZTkzNGElZDc3ZWNjIiwidGFnIjoiIn0%3D; expires=Tue, 18 Nov 2025 03:36:10 GMT; Max-Age=7200; path=/; secure; samesite=lax

set-cookie: **laravel_session**=eyJpdiI6ImJvVkZqRExGd0hvWXdsZm04bklOVkE9PSIsInZhbHVlIjoiUkpWbmk1aE03TmV1bTg1MTQvMHVGcG0vMUZrRlpMQ2Y3cWx5a29adkpWS0l2VmZDRjdheE9FMHp0NFNKb0F5K0VlWDltOHdn
U3FqTGd6Ym9kbDEvRDRiOGVicVdKR2M4ejlCSDAwanloSzVkZ0oyU0lmS2psOXJDQmp4b3F3VTQiLCJtYWMiOiI1NzhkNzQ2MjY3NDNmYWNhTk0MmJhMjFlMmQ2YjBlYTBmNWJmOTZlMDk1MzI1ZTQ5NjUxNmRjZTJkYzJiNDQ5IiwidGFn
IjoiIn0%3D; expires=Tue, 18 Nov 2025 03:36:10 GMT; Max-Age=7200; path=/; secure; httponly; samesite=lax
platform: hostinger
panel: hpanel
Content-Security-Policy: upgrade-insecure-requests
Server: hcdn
alt-svc: h3=":443"; ma=86400
x-hcdn-request-id: 4f489f24ae6ec7bc0e1d96f5bc550939-bos-edge4
x-hcdn-cache-status: DYNAMIC
x-hcdn-upstream-rt: 0.825
content-length: 32839

Response Body **(truncated)**	`<!DOCTYPE html>`
	`<html lang="en">`
	
	`<head>`
	`    <meta charset="UTF-8">`
	`    <meta name="viewport" content="width=device-width, initial-scale=1.0">`
	`    <title>Program Afiliasi IPWIJA</title>`
	`    <!-- Bootstrap CSS -->`
	`    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">`
	`    <link rel="preconnect" href="https://fonts.googleapis.com">`
	`    <link rel="preconnect" href="https://fonts.gstatic.com" crossorigin>`
	`    <link href="https://fonts.go...(truncated)`

URL	https://afiliasi.ipwija.ac.id/forgot-password
Method	GET
Parameter	laravel_session
Attack	
Evidence	laravel_session
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	https://afiliasi.ipwija.ac.id/login
Method	GET
Parameter	laravel_session
Attack	
Evidence	laravel_session
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	https://afiliasi.ipwija.ac.id/register
Method	GET
Parameter	laravel_session
Attack	
Evidence	laravel_session
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	SIAKAD_CLOUD_FRONT_ACCESS
Attack	
Evidence	SIAKAD_CLOUD_FRONT_ACCESS
Other Info	cookie:SIAKAD_CLOUD_FRONT_ACCESS
URL	https://afiliasi.ipwija.ac.id/storeRegister
Method	POST
Parameter	laravel_session
Attack	
Evidence	laravel_session
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	https://afiliasi.ipwija.ac.id/validateLogin
Method	POST
Parameter	laravel_session
Attack	
Evidence	laravel_session
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
Instances	7
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/
CWE Id	
WASC Id	
Plugin Id	10112

Informational	**User Controllable HTML Element Attribute (Potential XSS)**

Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://pmb.ipwija.ac.id/?lang=en
Method	GET
Parameter	lang
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://pmb.ipwija.ac.id/?lang=en appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=en The user-controlled value was: en
Request Header	GET https://pmb.ipwija.ac.id/?lang=en HTTP/1.1 host: pmb.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://pmb.ipwija.ac.id/ Cookie: SIAKAD_CLOUD_FRONT_ACCESS=1v8e8gfstl0q5ddfbrb3sojai9
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 18 Nov 2025 01:38:23 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache SX-Kode-PT: 1519 SX-Role: Peminat SX-User: SX-Session: 1v8e8gfstl0q5ddfbrb3sojai9 SX-Action: view Beranda SX-Action-Result: 1 SX-Message: SX-Referer: / Vary: Accept-Encoding content-length: 38227
Response Body **(truncated)**	<!DOCTYPE html> <html lang="en"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <!-- Load Base CSS --> <link rel="stylesheet" href="https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/css/bootstrap.min.css" /> <!-- Material Icons --> <link href="https://fonts.googleapis.com/css2?family=Material+Icons+Round" rel="stylesheet" /> <link href="ht...(truncated)
URL	https://pmb.ipwija.ac.id/home?lang=en
Method	GET
Parameter	lang
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://pmb.ipwija.ac.id/home?lang=en appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=en The user-controlled value was: en
URL	http://repository.ipwija.ac.id/cgi/register
Method	POST
Parameter	_action_register
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://repository.ipwija.ac.id/cgi/register appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _action_register=Register The user-controlled value was: register
URL	http://repository.ipwija.ac.id/cgi/register
Method	POST
Parameter	_action_register
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://repository.ipwija.ac.id/cgi/register appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _action_register=Register The user-controlled value was: register::internal
URL	http://repository.ipwija.ac.id/cgi/register
Method	POST
Parameter	_default_action
Attack	

Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://repository.ipwija.ac.id/cgi/register appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _default_action=register The user-controlled value was: register
URL	http://repository.ipwija.ac.id/cgi/register
Method	POST
Parameter	_default_action
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://repository.ipwija.ac.id/cgi/register appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _default_action=register The user-controlled value was: register::internal
URL	http://repository.ipwija.ac.id/cgi/register
Method	POST
Parameter	c1_name_family
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://repository.ipwija.ac.id/cgi/register appears to include user input in: a(n) [input] tag [value] attribute The user input found was: c1_name_family=ZAP The user-controlled value was: zap
URL	http://repository.ipwija.ac.id/cgi/register
Method	POST
Parameter	c1_name_given
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://repository.ipwija.ac.id/cgi/register appears to include user input in: a(n) [input] tag [value] attribute The user input found was: c1_name_given=ZAP The user-controlled value was: zap
URL	http://repository.ipwija.ac.id/cgi/register
Method	POST
Parameter	c1_name_honourific
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://repository.ipwija.ac.id/cgi/register appears to include user input in: a(n) [input] tag [value] attribute The user input found was: c1_name_honourific=ZAP The user-controlled value was: zap
URL	http://repository.ipwija.ac.id/cgi/register
Method	POST
Parameter	c1_newemail
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://repository.ipwija.ac.id/cgi/register appears to include user input in: a(n) [input] tag [value] attribute The user input found was: c1_newemail=ZAP The user-controlled value was: zap
URL	http://repository.ipwija.ac.id/cgi/register
Method	POST
Parameter	c1_newpassword
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://repository.ipwija.ac.id/cgi/register appears to include user input in: a(n) [input] tag [value] attribute The user input found was: c1_newpassword=ZAP The user-controlled value was: zap
URL	http://repository.ipwija.ac.id/cgi/register
Method	POST
Parameter	c1_username
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://repository.ipwija.ac.id/cgi/register appears to include user input in: a(n) [input] tag [value] attribute The user input found was: c1_username=ZAP The user-controlled value was: zap
URL	http://repository.ipwija.ac.id/cgi/register
Method	POST
Parameter	screen
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://repository.ipwija.ac.id/cgi/register appears to include user input in: a(n) [input] tag [value] attribute The user input found was: screen=Register::Internal The user-controlled value was: register::internal
Instances	13
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031