OWASP ZAP Scan Report

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

All scanned sites: http://ipwija.ac.id https://pmb.ipwija.ac.id http://repository.ipwija.ac.id https://afiliasi.ipwija.ac.id https://lp2m.ipwija.ac.id https://ipwija.ac.id

Javascript included from: https://www.google-analytics.com http://ipwija.ac.id https://pmb.ipwija.ac.id http://repository.ipwija.ac.id https://afiliasi.ipwija.ac.id https://lp2m.ipwija.ac.id https://ipwija.ac.id

Generated on Thu, 8 Jan 2026 02:04:08

ZAP Version: 2.17.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	10
Low	10
Informational	7

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	16
CSP: Failure to Define Directive with No Fallback	Medium	6
CSP: Wildcard Directive	Medium	6
CSP: script-src unsafe-inline	Medium	6
CSP: style-src unsafe-inline	Medium	6
Content Security Policy (CSP) Header Not Set	Medium	11
Missing Anti-clickjacking Header	Medium	20
Sub Resource Integrity Attribute Missing	Medium	17
Vulnerable JS Library	Medium	1
Weak Authentication Method	Medium	3
Big Redirect Detected (Potential Sensitive Information Leak)	Low	3
Cookie No HttpOnly Flag	Low	4
Cookie Without Secure Flag	Low	1
Cookie without SameSite Attribute	Low	6
Cross-Domain JavaScript Source File Inclusion	Low	7
In Page Banner Information Leak	Low	3
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	6
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	5
Strict-Transport-Security Header Not Set	Low	8
X-Content-Type-Options Header Missing	Low	8
Charset Mismatch	Informational	2
Content-Type Header Missing	Informational	1
Cookie Poisoning	Informational	3
Re-examine Cache-control Directives	Informational	8
Retrieved from Cache	Informational	5
Session Management Response Identified	Informational	7
User Controllable HTML Element Attribute (Potential XSS)	Informational	37

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ZAP is Out of Date	Passive	MEDIUM	-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	-
Java Serialization Object	Passive	MEDIUM	-
Application Error Disclosure	Passive	MEDIUM	-
Information Disclosure - Debug Error Messages	Passive	MEDIUM	-

Generated by HostedScan

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	-
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	-
Authentication Request Identified	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/141.0.0.0 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: Thu, 08 Jan 2026 01:58:26 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, <a href="reset_password">click here</a> 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"><a name="c1"></a><a name="name"></a><a name="newemail"></a><a name="username"></a><a name="newpassword"></a><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://ipwija.ac.id/events/workshop-digitalisasi-umkm-langkah-mudah-menuju-pemasaran-online/
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://lp2m.ipwija.ac.id/contoh-berita-1/
Method	GET
Parameter	
Attack	
Evidence	<form action="https://lp2m.ipwija.ac.id/wp-comments-post.php" method="post" id="ast-commentform" class="comment-form">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "author" "comment_parent" "comment_post_ID" "email" "submit" "url" "wp-comment-cookies-consent"].
URL	https://lp2m.ipwija.ac.id/contoh-berita-2/
Method	GET
Parameter	
Attack	
Evidence	<form action="https://lp2m.ipwija.ac.id/wp-comments-post.php" method="post" id="ast-commentform" class="comment-form">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "author" "comment_parent" "comment_post_ID" "email" "submit" "url" "wp-comment-cookies-consent"].
URL	https://lp2m.ipwija.ac.id/contoh-berita-3/
Method	GET
Parameter	
Attack	
Evidence	<form action="https://lp2m.ipwija.ac.id/wp-comments-post.php" method="post" id="ast-commentform" class="comment-form">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "author" "comment_parent" "comment_post_ID" "email" "submit" "url" "wp-comment-cookies-consent"].
URL	https://lp2m.ipwija.ac.id/contoh-berita-4/
Method	GET
Parameter	
Attack	
Evidence	<form action="https://lp2m.ipwija.ac.id/wp-comments-post.php" method="post" id="ast-commentform" class="comment-form">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "author" "comment_parent" "comment_post_ID" "email" "submit" "url" "wp-comment-cookies-consent"].
URL	https://lp2m.ipwija.ac.id/contoh-berita-5/
Method	GET
Parameter	
Attack	
Evidence	<form action="https://lp2m.ipwija.ac.id/wp-comments-post.php" method="post" id="ast-commentform" class="comment-form">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "author" "comment_parent" "comment_post_ID" "email" "submit" "url" "wp-comment-cookies-consent"].

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=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/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	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	16
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/141.0.0.0 Safari/537.36`
	`pragma: no-cache`
	`cache-control: no-cache`

Request Body	

Response Header	`HTTP/1.1 200 OK`
	`Date: Thu, 08 Jan 2026 01:57:35 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/"23241-1767328398;gz"`
	`X-LiteSpeed-Cache: hit`
	`platform: hostinger`
	`panel: hpanel`
	`Content-Security-Policy:` **`upgrade-insecure-requests`**
	`Age: 135`
	`Server: hcdn`
	`alt-svc: h3=":443"; ma=86400`
	`x-hcdn-request-id: 8195b563199d922df4d3be2b7c260d60-phx-edge7`
	`x-hcdn-cache-status: HIT`
	`content-length: 414114`

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/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/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/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://lp2m.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.
Instances	6
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/141.0.0.0 Safari/537.36`
	`pragma: no-cache`
	`cache-control: no-cache`

Request Body	

Response Header	`HTTP/1.1 200 OK`
	`Date: Thu, 08 Jan 2026 01:57:35 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/"23241-1767328398;gz"`
	`X-LiteSpeed-Cache: hit`
	`platform: hostinger`
	`panel: hpanel`
	`Content-Security-Policy:` **`upgrade-insecure-requests`**
	`Age: 135`
	`Server: hcdn`
	`alt-svc: h3=":443"; ma=86400`
	`x-hcdn-request-id: 8195b563199d922df4d3be2b7c260d60-phx-edge7`
	`x-hcdn-cache-status: HIT`
	`content-length: 414114`

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/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/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/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://lp2m.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
Instances	6
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/141.0.0.0 Safari/537.36`
	`pragma: no-cache`
	`cache-control: no-cache`

Request Body	

Response Header	`HTTP/1.1 200 OK`
	`Date: Thu, 08 Jan 2026 01:57:35 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/"23241-1767328398;gz"`
	`X-LiteSpeed-Cache: hit`
	`platform: hostinger`
	`panel: hpanel`
	`Content-Security-Policy: `**`upgrade-insecure-requests`**
	`Age: 135`

	Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 8195b563199d922df4d3be2b7c260d60-phx-edge7 x-hcdn-cache-status: HIT content-length: 414114

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/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/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/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://lp2m.ipwija.ac.id/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
Instances	6
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/141.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Date: Thu, 08 Jan 2026 01:57:35 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/"23241-1767328398;gz" X-LiteSpeed-Cache: hit platform: hostinger panel: hpanel Content-Security-Policy: **upgrade-insecure-requests** Age: 135 Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 8195b563199d922df4d3be2b7c260d60-phx-edge7 x-hcdn-cache-status: HIT content-length: 414114

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/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/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/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://lp2m.ipwija.ac.id/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.

Instances	6
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/141.0.0.0 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: Thu, 08 Jan 2026 01:57:42 GMT`
	`Server: Apache/2.4.29 (Ubuntu)`
	`Expires: Sat, 07 Feb 2026 01:57:42 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/information.html
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/divisions/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://repository.ipwija.ac.id/view/year/
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://afiliasi.ipwija.ac.id/
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/home
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	
Instances	11
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/141.0.0.0 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: Thu, 08 Jan 2026 01:57:42 GMT Server: Apache/2.4.29 (Ubuntu) Expires: Sat, 07 Feb 2026 01:57:42 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/information.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/year/
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/biaya-kuliah-universitas-ipwija/
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/simulasi-rapor/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://lp2m.ipwija.ac.id/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://lp2m.ipwija.ac.id/berita/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://lp2m.ipwija.ac.id/e-publikasi/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://lp2m.ipwija.ac.id/elementor-53/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://lp2m.ipwija.ac.id/pengumuman/
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/home
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	
Instances	20
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	**Sub Resource Integrity Attribute Missing**
Description	The integrity attribute is missing on a script or link tag served by an external server. The integrity tag prevents an attacker who have gained access to this server from injecting a malicious content.
URL	https://afiliasi.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	<link href="https://fonts.googleapis.com/css?family=DM+Sans:300,300i,400,400i,600,600i,700,700i,800,800i" rel="stylesheet">
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/141.0.0.0 Safari/537.36`
	`pragma: no-cache`
	`cache-control: no-cache`
	`referer: https://ipwija.ac.id/`

Request Body	

Response Header	`HTTP/1.1 404 Not Found`
	`Date: Thu, 08 Jan 2026 01:57:41 GMT`
	`Content-Type: text/html`
	`Connection: keep-alive`
	`Vary: Accept-Encoding`
	`Last-Modified: Tue, 22 Apr 2025 07:41:12 GMT`
	`Etag: W/"119f-68074818-9011dbc2cc1aa65c;gz"`
	`platform: hostinger`
	`panel: hpanel`
	`Server: hcdn`
	`alt-svc: h3=":443"; ma=86400`
	`x-hcdn-request-id: 34beb50e254807afc7d2d672c61c2d70-phx-edge7`
	`content-length: 4511`

Response Body **(excerpt)**	`th, initial-scale=1">`
	`    <title>This Page Does Not Exist</title>`
	`    <meta name="description" content="Oops, looks like the page is lost.">`
	`    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css">`
	`    <link href="https://fonts.googleapis.com/css?family=DM+Sans:300,300i,400,400i,600,600i,700,700i,800,800i"`
	`        rel="stylesheet">`
	`    <link href="https://fonts.googleapis.com/css?family=Roboto:300,300i,400,400i,600,600i,700,700i,800,800i"`
	`        rel="stylesheet">`
	
	`    <script type="text/javascript" async=""`
	`        src="https://www.googletagmanager.com/gtag/js?id=G-9Q6H0QETRF`

URL	https://afiliasi.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	<link href="https://fonts.googleapis.com/css?family=Roboto:300,300i,400,400i,600,600i,700,700i,800,800i" rel="stylesheet">
Other Info	
URL	https://afiliasi.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css">
Other Info	
URL	https://afiliasi.ipwija.ac.id/

Method	GET
Parameter	
Attack	
Evidence	<script async="" src="https://www.google-analytics.com/analytics.js"></script>
Other Info	
URL	https://afiliasi.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	<script type="text/javascript" async="" src="https://www.googletagmanager.com/gtag/js?id=G-9Q6H0QETRF&amp;cx=c&amp;_slc=1"></script>
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/chaty/js/cht-front-script.min.js?ver=3.4.11742195845
Method	GET
Parameter	
Attack	
Evidence	<link rel="preload" as="style" href="https://fonts.googleapis.com/css?family='+it+'&display=swap">
Other Info	
URL	https://ipwija.ac.id/wp-content/plugins/chaty/js/cht-front-script.min.js?ver=3.4.11742195845
Method	GET
Parameter	
Attack	
Evidence	<link rel="stylesheet" href="https://fonts.googleapis.com/css?family='+it+'&display=swap">
Other Info	
URL	https://lp2m.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	<link rel='stylesheet' id='astra-google-fonts-css' href='https://fonts.googleapis.com/css?family=Poppins%3A500&#038;display=fallback&#038;ver=4.9.2' media='all' />
Other Info	
URL	https://lp2m.ipwija.ac.id/berita/
Method	GET
Parameter	
Attack	
Evidence	<link rel='stylesheet' id='astra-google-fonts-css' href='https://fonts.googleapis.com/css?family=Poppins%3A500&#038;display=fallback&#038;ver=4.9.2' media='all' />
Other Info	
URL	https://lp2m.ipwija.ac.id/e-publikasi/
Method	GET
Parameter	
Attack	
Evidence	<link rel='stylesheet' id='astra-google-fonts-css' href='https://fonts.googleapis.com/css?family=Poppins%3A500&#038;display=fallback&#038;ver=4.9.2' media='all' />
Other Info	
URL	https://lp2m.ipwija.ac.id/elementor-53/
Method	GET
Parameter	
Attack	
Evidence	<link rel='stylesheet' id='astra-google-fonts-css' href='https://fonts.googleapis.com/css?family=Poppins%3A500&#038;display=fallback&#038;ver=4.9.2' media='all' />
Other Info	
URL	https://lp2m.ipwija.ac.id/pengumuman/
Method	GET
Parameter	
Attack	
Evidence	<link rel='stylesheet' id='astra-google-fonts-css' href='https://fonts.googleapis.com/css?family=Poppins%3A500&#038;display=fallback&#038;ver=4.9.2' media='all' />
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	<link href="https://fonts.googleapis.com/css2?family=Material+Icons" rel="stylesheet" />
Other Info	
URL	https://pmb.ipwija.ac.id/

Method	GET
Parameter	
Attack	
Evidence	<link href="https://fonts.googleapis.com/css2?family=Material+Icons+Outlined" rel="stylesheet" />
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	<link href="https://fonts.googleapis.com/css2?family=Material+Icons+Round" rel="stylesheet" />
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	<link rel="stylesheet" href="https://assets.siakadcloud.com/spmbfront/assets/v4/external/air-datepicker/css/datepicker.css" />
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	<link rel="stylesheet" href="https://assets.siakadcloud.com/spmbfront/assets/v4/external/dist/css/bootstrap.min.css" />
Other Info	
Instances	17
Solution	Provide a valid integrity attribute to the tag.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
CWE Id	[345](345)
WASC Id	15
Plugin Id	[90003](90003)

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/141.0.0.0 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: Thu, 08 Jan 2026 01:57:45 GMT`
	`Content-Type: application/x-javascript`
	`Connection: keep-alive`
	`Vary: Accept-Encoding`
	`Cache-Control: public, max-age=604800`
	`Expires: Thu, 15 Jan 2026 01:57:45 GMT`
	`Last-Modified: Fri, 14 Mar 2025 15:38:09 GMT`
	`Etag: W/"13a3a-67d44d61-c19d3abddce3d8cb;gz"`
	`platform: hostinger`
	`panel: hpanel`
	`Content-Security-Policy: upgrade-insecure-requests`
	`Server: hcdn`
	`alt-svc: h3=":443"; ma=86400`
	`x-hcdn-request-id: 5850c4b2aa68b953a63c458dc33fc4a3-phx-edge6`
	`x-hcdn-cache-status: MISS`
	`x-hcdn-upstream-rt: 0.633`
	`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/141.0.0.0 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: Thu, 08 Jan 2026 01:58:26 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> <h1>Unauthorized</h1> <p>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.</p> <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/141.0.0.0 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: Thu, 08 Jan 2026 01:57:49 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: d913af12cc177fedef936416482b799a-phx-edge8 x-hcdn-cache-status: MISS x-hcdn-upstream-rt: 0.495
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
Instances	3
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://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/141.0.0.0 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: Thu, 08 Jan 2026 01:57:42 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Server: Apache
Set-Cookie: SIAKAD_CLOUD_FRONT_ACCESS=paj46hps2uv72if9cs3e42lt75; 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: paj46hps2uv72if9cs3e42lt75
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)
```

URL	https://lp2m.ipwija.ac.id/wp-comments-post.php
Method	POST
Parameter	comment_author_761899d1b8e340a83bdd8219a7b3a227
Attack	
Evidence	set-cookie: comment_author_761899d1b8e340a83bdd8219a7b3a227
Other Info	
URL	https://lp2m.ipwija.ac.id/wp-comments-post.php
Method	POST
Parameter	comment_author_email_761899d1b8e340a83bdd8219a7b3a227
Attack	
Evidence	set-cookie: comment_author_email_761899d1b8e340a83bdd8219a7b3a227
Other Info	
URL	https://lp2m.ipwija.ac.id/wp-comments-post.php
Method	POST
Parameter	comment_author_url_761899d1b8e340a83bdd8219a7b3a227
Attack	
Evidence	set-cookie: comment_author_url_761899d1b8e340a83bdd8219a7b3a227
Other Info	
Instances	4
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/141.0.0.0 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: Thu, 08 Jan 2026 01:57:42 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Server: Apache
Set-Cookie: SIAKAD_CLOUD_FRONT_ACCESS=paj46hps2uv72if9cs3e42lt75; 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: paj46hps2uv72if9cs3e42lt75
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://lp2m.ipwija.ac.id/download/180/?tmstv=1767837525
Method	GET
Parameter	wp-dlm_cookie
Attack	
Evidence	set-cookie: wp-dlm_cookie
Other Info	

Request Header

```
GET https://lp2m.ipwija.ac.id/download/180/?tmstv=1767837525 HTTP/1.1
host: lp2m.ipwija.ac.id
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: https://lp2m.ipwija.ac.id/katalog_buku/manajemen-operasional-pengambilan-keputusan-strategis/
Cookie: comment_author_761899d1b8e340a83bdd8219a7b3a227=ZAP; comment_author_email_761899d1b8e340a83bdd8219a7b3a227=zaproxy%40example.com; comment_author_url_761899d1b8e340a83bdd8219a7b3a227=https%3A%2F%2Fzap.example.com; PHPSESSID=h1da3fhe5n6t245rvessvcg7nj
```

Request Body

Response Header

```
HTTP/1.1 200 OK
Date: Thu, 08 Jan 2026 02:00:45 GMT
Content-Type: application/pdf
Content-Length: 3673344
Connection: keep-alive
X-Powered-By: PHP/8.2.28
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
set-cookie: wp-dlm_cookie=1edb0e8ff29a54e94d75b6ca6f3064ba; expires=Thu, 08 Jan 2026 02:01:45 GMT; Max-Age=60; path=/; secure; HttpOnly
X-LiteSpeed-Cache-Control: no-cache
Content-Disposition: attachment; filename*=UTF-8''Manajemen-Operasional-Pengambilan-Keputusan-Strategis.pdf;
X-Robots-Tag: noindex, nofollow
Content-Description: File Transfer
```

	Content-Transfer-Encoding: binary Cache-Control: no-store, no-cache, must-revalidate, no-transform, max-age=0 X-DLM-Filesize: 3673344 platform: hostinger panel: hpanel Content-Security-Policy: upgrade-insecure-requests Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 2e774bc0ff63da820b0723eaa752f0a1-phx-edge8 x-hcdn-cache-status: DYNAMIC x-hcdn-upstream-rt: 0.712 Accept-Ranges: bytes
Response Body **(truncated)**	%PDF-1.7 %âãÏÓ 2304 0 obj <</Names 2305 0 R/Outlines 1023 0 R/Metadata 2331 0 R/AcroForm 2327 0 R/Pages 2260 0 R/OCProperties<</D<</RBGroups[]/OFF[]/Order[[(000#000 cvr blkng.pdf)2306 0 R]]>>/OCGs[2306 0 R]>>/StructTreeRoot 1375 0 R/Type/Catalog>> endobj 2305 0 obj <</Dests 2258 0 R>> endobj 1023 0 obj <</First 1024 0 R/Count 176/Last 1025 0 R>> endobj 2331 0 obj <</Subtype/XML/Length 3634/Type/Metadata>>stream <?xpacket begin="ï»¿" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:...(truncated)
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://lp2m.ipwija.ac.id/wp-comments-post.php
Method	POST
Parameter	_lscache_vary
Attack	
Evidence	set-cookie: _lscache_vary
Other Info	
URL	https://lp2m.ipwija.ac.id/wp-comments-post.php
Method	POST
Parameter	comment_author_761899d1b8e340a83bdd8219a7b3a227
Attack	
Evidence	set-cookie: comment_author_761899d1b8e340a83bdd8219a7b3a227
Other Info	
URL	https://lp2m.ipwija.ac.id/wp-comments-post.php
Method	POST
Parameter	comment_author_email_761899d1b8e340a83bdd8219a7b3a227
Attack	
Evidence	set-cookie: comment_author_email_761899d1b8e340a83bdd8219a7b3a227
Other Info	
URL	https://lp2m.ipwija.ac.id/wp-comments-post.php
Method	POST
Parameter	comment_author_url_761899d1b8e340a83bdd8219a7b3a227
Attack	
Evidence	set-cookie: comment_author_url_761899d1b8e340a83bdd8219a7b3a227
Other Info	
Instances	6
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://www.google-analytics.com/analytics.js

<table>
<tr><td>Attack</td><td></td></tr>
<tr><td>Evidence</td><td><script async="" src="https://www.google-analytics.com/analytics.js"></script></td></tr>
<tr><td>Other Info</td><td></td></tr>
<tr><td>Request Header</td><td>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/141.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: https://ipwija.ac.id/</td></tr>
<tr><td>Request Body</td><td></td></tr>
<tr><td>Response Header</td><td>HTTP/1.1 404 Not Found
Date: Thu, 08 Jan 2026 01:57:41 GMT
Content-Type: text/html
Connection: keep-alive
Vary: Accept-Encoding
Last-Modified: Tue, 22 Apr 2025 07:41:12 GMT
Etag: W/"119f-68074818-9011dbc2cc1aa65c;gz"
platform: hostinger
panel: hpanel
Server: hcdn
alt-svc: h3=":443"; ma=86400
x-hcdn-request-id: 34beb50e254807afc7d2d672c61c2d70-phx-edge7
content-length: 4511</td></tr>
<tr><td>Response Body **(excerpt)**</td><td>eapis.com/css?family=Roboto:300,300i,400,400i,600,600i,700,700i,800,800i"
        rel="stylesheet">

    <script type="text/javascript" async=""
        src="https://www.googletagmanager.com/gtag/js?id=G-9Q6H0QETRF&amp;cx=c&amp;_slc=1"></script>
    <script async="" src="https://www.google-analytics.com/analytics.js"></script>
    <script>
        (function (i, s, o, g, r, a, m) {
            i['GoogleAnalyticsObject'] = r; i[r] = i[r] || function () {
                (i[r].q = i[r].q || []).push(arguments)
            }, i[r].l = 1 * new Date(); a = s.createElement(o),</td></tr>
<tr><td>URL</td><td>https://afiliasi.ipwija.ac.id/</td></tr>
<tr><td>Method</td><td>GET</td></tr>
<tr><td>Parameter</td><td>https://www.googletagmanager.com/gtag/js?id=G-9Q6H0QETRF&cx=c&_slc=1</td></tr>
<tr><td>Attack</td><td></td></tr>
<tr><td>Evidence</td><td><script type="text/javascript" async="" src="https://www.googletagmanager.com/gtag/js?id=G-9Q6H0QETRF&amp;cx=c&amp;_slc=1"></script></td></tr>
<tr><td>Other Info</td><td></td></tr>
<tr><td>URL</td><td>https://pmb.ipwija.ac.id/</td></tr>
<tr><td>Method</td><td>GET</td></tr>
<tr><td>Parameter</td><td>https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js</td></tr>
<tr><td>Attack</td><td></td></tr>
<tr><td>Evidence</td><td><script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js"></script></td></tr>
<tr><td>Other Info</td><td></td></tr>
<tr><td>URL</td><td>https://pmb.ipwija.ac.id/</td></tr>
<tr><td>Method</td><td>GET</td></tr>
<tr><td>Parameter</td><td>https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js</td></tr>
<tr><td>Attack</td><td></td></tr>
<tr><td>Evidence</td><td><script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/bootstrap-datetimepicker.js"></script></td></tr>
<tr><td>Other Info</td><td></td></tr>
<tr><td>URL</td><td>https://pmb.ipwija.ac.id/</td></tr>
<tr><td>Method</td><td>GET</td></tr>
<tr><td>Parameter</td><td>https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js</td></tr>
<tr><td>Attack</td><td></td></tr>
<tr><td>Evidence</td><td><script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery-migrate-1.2.1.min.js"></script></td></tr>
<tr><td>Other Info</td><td></td></tr>
<tr><td>URL</td><td>https://pmb.ipwija.ac.id/</td></tr>
<tr><td>Method</td><td>GET</td></tr>
<tr><td>Parameter</td><td>https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js</td></tr>
<tr><td>Attack</td><td></td></tr>
<tr><td>Evidence</td><td><script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/jquery.min.js"></script></td></tr>
<tr><td>Other Info</td><td></td></tr>
<tr><td>URL</td><td>https://pmb.ipwija.ac.id/</td></tr>
<tr><td>Method</td><td>GET</td></tr>
<tr><td>Parameter</td><td>https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js</td></tr>
</table>

Attack	
Evidence	<script src="https://assets.siakadcloud.com/spmbfront/assets/v4/../default/js/moment.js"></script>
Other Info	
Instances	7
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	**In Page Banner Information Leak**
Description	The server returned a version banner string in the response content. Such information leaks may allow attackers to further target specific issues impacting the product and version in use.
URL	http://repository.ipwija.ac.id/cgi/users/home
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29
Other Info	There is a chance that the highlight in the finding is on a value in the headers, versus the actual matched string in the response body.
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/141.0.0.0 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: Thu, 08 Jan 2026 01:58:26 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 **(excerpt)**	> <p>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.</p> <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	Apache/2.4.29
Other Info	There is a chance that the highlight in the finding is on a value in the headers, versus the actual matched string in the response body.
URL	http://repository.ipwija.ac.id/sword-app/servicedocument
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.29
Other Info	There is a chance that the highlight in the finding is on a value in the headers, versus the actual matched string in the response body.
Instances	3
Solution	Configure the server to prevent such information leaks. For example: Under Tomcat this is done via the "server" directive and implementation of custom error pages. Under Apache this is done via the "ServerSignature" and "ServerTokens" directives.
Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/08-Testing_for_Error_Handling/
CWE Id	497
WASC Id	13
Plugin Id	10009

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://ipwija.ac.id/

Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
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/141.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Date: Thu, 08 Jan 2026 01:57:35 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/"23241-1767328398;gz" X-LiteSpeed-Cache: hit platform: hostinger panel: hpanel Content-Security-Policy: upgrade-insecure-requests Age: 135 Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 8195b563199d922df4d3be2b7c260d60-phx-edge7 x-hcdn-cache-status: HIT content-length: 414114

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/informasi-beasiswa/
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/wp-json/
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://lp2m.ipwija.ac.id/
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.28
Other Info	
Instances	6
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/141.0.0.0 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: Thu, 08 Jan 2026 01:57:42 GMT`
	`Server:` **`Apache/2.4.29 (Ubuntu)`**
	`Expires: Sat, 07 Feb 2026 01:57:42 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/information.html
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/divisions/
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	
Instances	5
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/141.0.0.0 Safari/537.36`
	`pragma: no-cache`
	`cache-control: no-cache`
	`referer: https://ipwija.ac.id/`

Request Body	

Response Header	`HTTP/1.1 404 Not Found`
	`Date: Thu, 08 Jan 2026 01:57:41 GMT`
	`Content-Type: text/html`
	`Connection: keep-alive`
	`Vary: Accept-Encoding`
	`Last-Modified: Tue, 22 Apr 2025 07:41:12 GMT`
	`Etag: W/"119f-68074818-9011dbc2cc1aa65c;gz"`
	`platform: hostinger`
	`panel: hpanel`
	`Server: hcdn`
	`alt-svc: h3=":443"; ma=86400`
	`x-hcdn-request-id: 34beb50e254807afc7d2d672c61c2d70-phx-edge7`
	`content-length: 4511`

Response Body **(truncated)**	`<!DOCTYPE html>`
	`<html lang="en-us"`
	` prefix="content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs: http://www.w3.org/2000/01/rdf-schema# sioc: http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd: http://www.w3.org/2001/XMLSchema#">`
	
	`<head>`
	`    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">`
	`    <style type="text/css">`
	`        @charset...(truncated)`

URL	https://ipwija.ac.id/
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/robots.txt
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/wp/v2/pages/15509
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://lp2m.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://pmb.ipwija.ac.id/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	8
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/141.0.0.0 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: Thu, 08 Jan 2026 01:57:42 GMT Server: Apache/2.4.29 (Ubuntu) Expires: Sat, 07 Feb 2026 01:57:42 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://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/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/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/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/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://lp2m.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://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	8
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	**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/141.0.0.0 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: Thu, 08 Jan 2026 01:57:43 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/"25264-1767837463;gz" X-Litespeed-Cache: miss platform: hostinger panel: hpanel Content-Security-Policy: upgrade-insecure-requests Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: ed9b8d23d5ccca86a3e2a36d26968acd-phx-edge8 x-hcdn-cache-status: MISS x-hcdn-upstream-rt: 0.760 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>&lt;blockquote class="wp-embedded-content" data-secret="ZtyN8Auhrh"&gt;&lt;a href="https://ipwija.ac.id/"&gt;University&lt;/a&gt;&lt;/blockquote&gt;&lt;iframe sandb...(truncated)
URL	https://lp2m.ipwija.ac.id/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Flp2m.ipwija.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.
Instances	2
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/archive/p/browsersec/wikis/Part2.wiki#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011

Informational	**Content-Type Header Missing**
Description	The Content-Type header was either missing or empty.
URL	https://pmb.ipwija.ac.id/uploads/ipwija/filepengumumanspmb/1
Method	GET
Parameter	content-type
Attack	
Evidence	
Other Info	
Request Header	GET https://pmb.ipwija.ac.id/uploads/ipwija/filepengumumanspmb/1 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/141.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://pmb.ipwija.ac.id/detail-pengumuman/3/brosur-pmb-20252026 Cookie: SIAKAD_CLOUD_FRONT_ACCESS=paj46hps2uv72if9cs3e42lt75
Request Body	
Response Header	HTTP/1.1 200 OK Date: Thu, 08 Jan 2026 02:00:36 GMT Content-Length: 763854 Connection: keep-alive Server: Apache Last-Modified: Mon, 28 Apr 2025 06:17:47 GMT ETag: "ba7ce-633d0a498cf20"

	Accept-Ranges: bytes sx-svc: w5
Response Body **(truncated)**	ÿØÿà□JFIF□□□□ÿÛC□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □ □ □ □□□ □ □□□□□□ □□□□□□□□□ÿÛC□□□□□□□□□□□□□□□□ □□□ÿÀ□□□j□@□□□□□□□□□□ÿÄ□□□□□□□□□□□□□□□□□□□□□□□□□□ □ÿÄµ□□□□□□□□□□□□□□□}□□□□□□□!1A□□Qa□"q□2□□¡□#B±Á□RÑð$3br□ □□□□□%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz□□□□□□□□□□□□□□□□□□□□□¢£¤¥¦§¨©ª²³´µ¶·¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚáâãäåæçèéêñòóôõö÷øùúÿÄ□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □ÿÄµ□□□□□□□□□□□□□□□□w□□□□□□!1□□AQ□aq□"2□□□B□¡±Á #3Rð□brÑ □$4á%ñ□□□□&'()*5...(truncated)
Instances	1
Solution	Ensure each page is setting the specific and appropriate content-type value for the content being delivered.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)
CWE Id	345
WASC Id	12
Plugin Id	10019
Informational	**Cookie Poisoning**
Description	This check looks at user-supplied input in query string parameters and POST data to identify where cookie parameters might be controlled. This is called a cookie poisoning attack, and becomes exploitable when an attacker can manipulate the cookie in various ways. In some cases this will not be exploitable, however, allowing URL parameters to set cookie values is generally considered a bug.
URL	https://lp2m.ipwija.ac.id/wp-comments-post.php
Method	POST
Parameter	author
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: https://nottrusted.com/page?value=maliciousInput. This was identified at: https://lp2m.ipwija.ac.id/wp-comments-post.php User-input was found in the following cookie: comment_author_761899d1b8e340a83bdd8219a7b3a227=ZAP; expires=Fri, 08 Jan 2027 01:58:47 GMT; Max-Age=31536000; path=/; secure The user input was: author=ZAP
Request Header	POST https://lp2m.ipwija.ac.id/wp-comments-post.php HTTP/1.1 host: lp2m.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache content-type: application/x-www-form-urlencoded referer: https://lp2m.ipwija.ac.id/contoh-berita-5/ content-length: 216

Request Body	comment=Zaproxy+dolore+alias+impedit+expedita+quisquam.&author=ZAP&email=zaproxy%40example.com&url=https%3A%2F%2Fzap.example.com&wp-comment-cookies-consent=yes&submit=Post+Comment&
	comment_post_ID=230&comment_parent=0

Response Header	HTTP/1.1 302 Found Date: Thu, 08 Jan 2026 01:58:48 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: keep-alive X-Powered-By: PHP/8.2.28 Expires: Wed, 11 Jan 1984 05:00:00 GMT set-cookie: comment_author_761899d1b8e340a83bdd8219a7b3a227=ZAP; expires=Fri, 08 Jan 2027 01:58:47 GMT; Max-Age=31536000; path=/; secure set-cookie: comment_author_email_761899d1b8e340a83bdd8219a7b3a227=zaproxy%40example.com; expires=Fri, 08 Jan 2027 01:58:47 GMT; Max-Age=31536000; path=/; secure set-cookie: comment_author_url_761899d1b8e340a83bdd8219a7b3a227=https%3A%2F%2Fzap.example.com; expires=Fri, 08 Jan 2027 01:58:47 GMT; Max-Age=31536000; path=/; secure set-cookie: _lscache_vary=commenter; expires=Mon, 21 Dec 2026 07:18:47 GMT; Max-Age=30000000; path=/contoh-berita-5/; secure; HttpOnly X-Redirect-By: WordPress Location: https://lp2m.ipwija.ac.id/contoh-berita-5/#comment-2 X-LiteSpeed-Cache-Control: no-cache Cache-Control: no-cache, no-store, must-revalidate, max-age=0 platform: hostinger panel: hpanel Content-Security-Policy: upgrade-insecure-requests Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: e5f15bda4bcc329fa9847a1900f693be-phx-edge5 x-hcdn-cache-status: DYNAMIC x-hcdn-upstream-rt: 1.172
Response Body	
URL	https://lp2m.ipwija.ac.id/wp-comments-post.php
Method	POST
Parameter	email
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: https://nottrusted.com/page?value=maliciousInput. This was identified at: https://lp2m.ipwija.ac.id/wp-comments-post.php User-input was found in the following cookie: comment_author_email_761899d1b8e340a83bdd8219a7b3a227=zaproxy@example.com; expires=Fri, 08 Jan 2027 01:58:47 GMT; Max-Age=31536000; path=/; secure The user input was: email=zaproxy@example.com
URL	https://lp2m.ipwija.ac.id/wp-comments-post.php
Method	POST

Parameter	url
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: https://nottrusted.com/page?value=maliciousInput. This was identified at: https://lp2m.ipwija.ac.id/wp-comments-post.php User-input was found in the following cookie: comment_author_url_761899d1b8e340a83bdd8219a7b3a227=https://zap.example.com; expires=Fri, 08 Jan 2027 01:58:47 GMT; Max-Age=31536000; path=/; secure The user input was: url=https://zap.example.com
Instances	3
Solution	Do not allow user input to control cookie names and values. If some query string parameters must be set in cookie values, be sure to filter out semicolon's that can serve as name/value pair delimiters.
Reference	https://en.wikipedia.org/wiki/HTTP_cookie https://cwe.mitre.org/data/definitions/565.html
CWE Id	565
WASC Id	20
Plugin Id	10029

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://ipwija.ac.id/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
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/141.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Date: Thu, 08 Jan 2026 01:57:35 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/"23241-1767328398;gz" X-LiteSpeed-Cache: hit platform: hostinger panel: hpanel Content-Security-Policy: upgrade-insecure-requests Age: 135 Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 8195b563199d922df4d3be2b7c260d60-phx-edge7 x-hcdn-cache-status: HIT content-length: 414114

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/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/robots.txt
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://lp2m.ipwija.ac.id/
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=604800
Other Info	
URL	https://lp2m.ipwija.ac.id/berita/
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=604800
Other Info	
URL	https://lp2m.ipwija.ac.id/pengumuman/
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=604800
Other Info	
Instances	8
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: 135
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/141.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Date: Thu, 08 Jan 2026 01:57:35 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/"23241-1767328398;gz"
X-LiteSpeed-Cache: hit
platform: hostinger
panel: hpanel
Content-Security-Policy: upgrade-insecure-requests
Age: 135
Server: hcdn
alt-svc: h3=":443"; ma=86400
x-hcdn-request-id: 8195b563199d922df4d3be2b7c260d60-phx-edge7
x-hcdn-cache-status: HIT
content-length: 414114
```

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/
Method	GET
Parameter	
Attack	
Evidence	Age: 410
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/banjir-di-bekasi-civitas-ipwija-gotong-royong-pulihkan-lingkungan/
Method	GET
Parameter	
Attack	
Evidence	Age: 28651
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: 91281
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: 84754
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	5
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://lp2m.ipwija.ac.id/download/180/?tmstv=1767837525
Method	GET
Parameter	wp-dlm_cookie

Attack	
Evidence	wp-dlm_cookie
Other Info	cookie:wp-dlm_cookie
Request Header	GET https://lp2m.ipwija.ac.id/download/180/?tmstv=1767837525 HTTP/1.1 host: lp2m.ipwija.ac.id user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://lp2m.ipwija.ac.id/katalog_buku/manajemen-operasional-pengambilan-keputusan-strategis/ Cookie: comment_author_761899d1b8e340a83bdd8219a7b3a227=ZAP; comment_author_email_761899d1b8e340a83bdd8219a7b3a227=zaproxy%40example.com; comment_author_url_761899d1b8e340a83bdd8219a7b3a227=https%3A%2F%2Fzap.example.com; PHPSESSID=h1da3fhe5n6t245rvessvcg7nj
Request Body	
Response Header	HTTP/1.1 200 OK Date: Thu, 08 Jan 2026 02:00:45 GMT Content-Type: application/pdf Content-Length: 3673344 Connection: keep-alive X-Powered-By: PHP/8.2.28 Expires: Thu, 19 Nov 1981 08:52:00 GMT Pragma: no-cache set-cookie: **wp-dlm_cookie**=1edb0e8ff29a54e94d75b6ca6f3064ba; expires=Thu, 08 Jan 2026 02:01:45 GMT; Max-Age=60; path=/; secure; HttpOnly X-LiteSpeed-Cache-Control: no-cache Content-Disposition: attachment; filename*=UTF-8''Manajemen-Operasional-Pengambilan-Keputusan-Strategis.pdf; X-Robots-Tag: noindex, nofollow Content-Description: File Transfer Content-Transfer-Encoding: binary Cache-Control: no-store, no-cache, must-revalidate, no-transform, max-age=0 X-DLM-Filesize: 3673344 platform: hostinger panel: hpanel Content-Security-Policy: upgrade-insecure-requests Server: hcdn alt-svc: h3=":443"; ma=86400 x-hcdn-request-id: 2e774bc0ff63da820b0723eaa752f0a1-phx-edge8 x-hcdn-cache-status: DYNAMIC x-hcdn-upstream-rt: 0.712 Accept-Ranges: bytes
Response Body **(truncated)**	%PDF-1.7 %âãÏÓ 2304 0 obj <</Names 2305 0 R/Outlines 1023 0 R/Metadata 2331 0 R/AcroForm 2327 0 R/Pages 2260 0 R/OCProperties<</D<</RBGroups[]/OFF[]/Order[[(000#000 cvr blkng.pdf)2306 0 R]]>>/OCGs[2306 0 R]>>/StructTreeRoot 1375 0 R/Type/Catalog>> endobj 2305 0 obj <</Dests 2258 0 R>> endobj 1023 0 obj <</First 1024 0 R/Count 176/Last 1025 0 R>> endobj 2331 0 obj <</Subtype/XML/Length 3634/Type/Metadata>>stream <?xpacket begin="ï»¿" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:...(truncated)
URL	https://lp2m.ipwija.ac.id/no-access/embed/
Method	GET
Parameter	PHPSESSID
Attack	
Evidence	PHPSESSID
Other Info	cookie:PHPSESSID
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://lp2m.ipwija.ac.id/wp-comments-post.php
Method	POST
Parameter	comment_author_email_761899d1b8e340a83bdd8219a7b3a227
Attack	
Evidence	comment_author_email_761899d1b8e340a83bdd8219a7b3a227
Other Info	cookie:comment_author_email_761899d1b8e340a83bdd8219a7b3a227 cookie:comment_author_url_761899d1b8e340a83bdd8219a7b3a227
URL	https://lp2m.ipwija.ac.id/download/170/?tmstv=1767837525
Method	GET
Parameter	PHPSESSID
Attack	
Evidence	PHPSESSID

Other Info	cookie:PHPSESSID
URL	https://lp2m.ipwija.ac.id/download/170/?tmstv=1767837525
Method	GET
Parameter	wp-dlm_cookie
Attack	
Evidence	wp-dlm_cookie
Other Info	cookie:wp-dlm_cookie
URL	https://lp2m.ipwija.ac.id/wp-comments-post.php
Method	POST
Parameter	comment_author_url_761899d1b8e340a83bdd8219a7b3a227
Attack	
Evidence	comment_author_url_761899d1b8e340a83bdd8219a7b3a227
Other Info	cookie:comment_author_url_761899d1b8e340a83bdd8219a7b3a227
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	http://repository.ipwija.ac.id/cgi/search/simple?_action_search=Search&_order=bytitle&_satisfyall=ALL&basic_srchtype=ALL&q=ZAP
Method	GET
Parameter	_action_search
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/search/simple?_action_search=Search&_order=bytitle&_satisfyall=ALL&basic_srchtype=ALL&q=ZAP appears to include user input in: a(n) [link] tag [rel] attribute The user input found was: _action_search=Search The user-controlled value was: search
Request Header	GET http://repository.ipwija.ac.id/cgi/search/simple?_action_search=Search&_order=bytitle&_satisfyall=ALL&basic_srchtype=ALL&q=ZAP 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/141.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: http://repository.ipwija.ac.id/cgi/search?_action_search=Search&_order=bytitle&_satisfyall=ALL&basic_srchtype=ALL&q=ZAP
Request Body	
Response Header	HTTP/1.1 200 OK Date: Thu, 08 Jan 2026 01:59:08 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: 17330

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>Search results for ZAP - 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" />
	    <script type="text/javascript">
	// <![CDATA[
	var e...(truncated)

URL	http://repository.ipwija.ac.id/cgi/search/simple?_action_search=Search&_order=bytitle&_satisfyall=ALL&basic_srchtype=ALL&q=ZAP
Method	GET
Parameter	_order
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/search/simple?_action_search=Search&_order=bytitle&_satisfyall=ALL&basic_srchtype=ALL&q=ZAP appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _order=bytitle The user-controlled value was: bytitle
URL	http://repository.ipwija.ac.id/cgi/search/simple?_action_search=Search&_order=bytitle&_satisfyall=ALL&basic_srchtype=ALL&q=ZAP
Method	GET
Parameter	_satisfyall
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/search/simple?_action_search=Search&_order=bytitle&_satisfyall=ALL&basic_srchtype=ALL&q=ZAP appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _satisfyall=ALL The user-controlled value was: all

URL	http://repository.ipwija.ac.id/cgi/search/simple?_action_search=Search&_order=bytitle&_satisfyall=ALL&basic_srchtype=ALL&q=ZAP
Method	GET
Parameter	basic_srchtype
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/search/simple?_action_search=Search&_order=bytitle&_satisfyall=ALL&basic_srchtype=ALL&q=ZAP appears to include user input in: a(n) [input] tag [value] attribute The user input found was: basic_srchtype=ALL The user-controlled value was: all
URL	https://lp2m.ipwija.ac.id/unit-penerbitan-buku/?asl_gen%5B%5D=exact&customset%5B%5D=katalog_buku&filters_changed=0&filters_initial=1&phrase&qtranslate_lang=0
Method	GET
Parameter	asl_gen[]
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://lp2m.ipwija.ac.id/unit-penerbitan-buku/?asl_gen%5B%5D=exact&customset%5B%5D=katalog_buku&filters_changed=0&filters_initial=1&phrase&qtranslate_lang=0 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: asl_gen[]=exact The user-controlled value was: exact
URL	https://lp2m.ipwija.ac.id/unit-penerbitan-buku/?asl_gen%5B%5D=exact&customset%5B%5D=katalog_buku&filters_changed=0&filters_initial=1&phrase&qtranslate_lang=0
Method	GET
Parameter	customset[]
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://lp2m.ipwija.ac.id/unit-penerbitan-buku/?asl_gen%5B%5D=exact&customset%5B%5D=katalog_buku&filters_changed=0&filters_initial=1&phrase&qtranslate_lang=0 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: customset[]=katalog_buku The user-controlled value was: katalog_buku
URL	https://lp2m.ipwija.ac.id/unit-penerbitan-buku/?asl_gen%5B%5D=exact&customset%5B%5D=katalog_buku&filters_changed=0&filters_initial=1&phrase&qtranslate_lang=0
Method	GET
Parameter	filters_initial
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://lp2m.ipwija.ac.id/unit-penerbitan-buku/?asl_gen%5B%5D=exact&customset%5B%5D=katalog_buku&filters_changed=0&filters_initial=1&phrase&qtranslate_lang=0 appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: filters_initial=1 The user-controlled value was: width=device-width, initial-scale=1
URL	https://lp2m.ipwija.ac.id/unit-penerbitan-buku/?asl_gen%5B%5D=exact&customset%5B%5D=katalog_buku&filters_changed=0&filters_initial=1&qtranslate_lang=0
Method	GET
Parameter	asl_gen[]
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://lp2m.ipwija.ac.id/unit-penerbitan-buku/?asl_gen%5B%5D=exact&customset%5B%5D=katalog_buku&filters_changed=0&filters_initial=1&qtranslate_lang=0 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: asl_gen[]=exact The user-controlled value was: exact
URL	https://lp2m.ipwija.ac.id/unit-penerbitan-buku/?asl_gen%5B%5D=exact&customset%5B%5D=katalog_buku&filters_changed=0&filters_initial=1&qtranslate_lang=0
Method	GET
Parameter	customset[]
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://lp2m.ipwija.ac.id/unit-penerbitan-buku/?asl_gen%5B%5D=exact&customset%5B%5D=katalog_buku&filters_changed=0&filters_initial=1&qtranslate_lang=0 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: customset[]=katalog_buku The user-controlled value was: katalog_buku
URL	https://lp2m.ipwija.ac.id/unit-penerbitan-buku/?asl_gen%5B%5D=exact&customset%5B%5D=katalog_buku&filters_changed=0&filters_initial=1&qtranslate_lang=0
Method	GET
Parameter	filters_initial
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://lp2m.ipwija.ac.id/unit-penerbitan-buku/?asl_gen%5B%5D=exact&customset%5B%5D=katalog_buku&filters_changed=0&filters_initial=1&qtranslate_lang=0 appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: filters_initial=1 The user-controlled value was: width=device-width, initial-scale=1
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
URL	https://pmb.ipwija.ac.id/detail-pengumuman/3/brosur-pmb-20252026?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/detail-pengumuman/3/brosur-pmb-20252026?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	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	https://pmb.ipwija.ac.id/jalur-seleksi?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/jalur-seleksi?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	https://pmb.ipwija.ac.id/login?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/login?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	https://pmb.ipwija.ac.id/pengumuman?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/pengumuman?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	https://pmb.ipwija.ac.id/program-studi?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/program-studi?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	https://pmb.ipwija.ac.id/program-studi-detail/detail/15401?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/program-studi-detail/detail/15401?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	https://pmb.ipwija.ac.id/program-studi-detail/detail/55201?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/program-studi-detail/detail/55201?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	https://pmb.ipwija.ac.id/program-studi-detail/detail/57201?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/program-studi-detail/detail/57201?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	https://pmb.ipwija.ac.id/program-studi-detail/detail/59202?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/program-studi-detail/detail/59202?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	https://pmb.ipwija.ac.id/program-studi-detail/detail/61101?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/program-studi-detail/detail/61101?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	https://pmb.ipwija.ac.id/program-studi-detail/detail/61201?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/program-studi-detail/detail/61201?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	https://pmb.ipwija.ac.id/program-studi-detail/detail/94202?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/program-studi-detail/detail/94202?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	https://pmb.ipwija.ac.id/user-guide?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/user-guide?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::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::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
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	POST
Parameter	act
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/jalur-seleksi appears to include user input in: a(n) [input] tag [value] attribute The user input found was: act=reset The user-controlled value was: reset
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	POST
Parameter	jenjang
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/jalur-seleksi appears to include user input in: a(n) [option] tag [value] attribute The user input found was: jenjang=D3 The user-controlled value was: d3
URL	https://pmb.ipwija.ac.id/jalur-seleksi
Method	POST
Parameter	unit
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/jalur-seleksi appears to include user input in: a(n) [option] tag [value] attribute The user input found was: unit=15401 The user-controlled value was: 15401
Instances	37
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