ZAP by Checkmarx Scanning Report

Sites: http://bajajamc.dev.diginnovators.site https://bajajamc.dev.diginnovators.site

Generated on Wed, 21 Jan 2026 19:32:27

ZAP Version: 2.17.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	7
Low	4
Informational	6

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	5
CSP: Failure to Define Directive with No Fallback	Medium	5
CSP: Wildcard Directive	Medium	5
CSP: script-src unsafe-inline	Medium	5
CSP: style-src unsafe-inline	Medium	5
Content Security Policy (CSP) Header Not Set	Medium	5
Sub Resource Integrity Attribute Missing	Medium	5
Cookie without SameSite Attribute	Low	5
Cross-Domain JavaScript Source File Inclusion	Low	5
Secure Pages Include Mixed Content	Low	5
Timestamp Disclosure - Unix	Low	5
Charset Mismatch	Informational	1
Information Disclosure - Suspicious Comments	Informational	13
Modern Web Application	Informational	5
Re-examine Cache-control Directives	Informational	5
Session Management Response Identified	Informational	5
User Controllable HTML Element Attribute (Potential XSS)	Informational	290

Alert Detail

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

Description	A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL /form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://bajajamc.dev.diginnovators.site/
Method	GET
Attack	
Evidence	<form class="elementor-form" method="post" id="get_a_call_back" name="getacallback" aria-label="getacallback">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "form-field-country_code" "form-field-email" "form-field-mobile_number" "form-field-name" "form_id" "post_id" "queried_id" "referer_title"].
URL	https://bajajamc.dev.diginnovators.site/contact-us/
Method	GET
Attack	
Evidence	<form class="elementor-form" method="post" id="get_a_call_back" name="getacallback" aria-label="getacallback">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "form-field-country_code" "form-field-email" "form-field-mobile_number" "form-field-name" "form_id" "post_id" "queried_id" "referer_title"].
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/?e-filter-ccaa784-glossary-type=mutual-fund&e-filter-e0a7636-category=wealth-creation
Method	GET
Attack	
Evidence	<form class="elementor-form" method="post" id="get_a_call_back" name="getacallback" aria-label="getacallback">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "form-field-country_code" "form-field-email" "form-field-mobile_number" "form-field-name" "form_id" "post_id" "queried_id" "referer_title"].
URL	https://bajajamc.dev.diginnovators.site/sip/
Method	GET
Attack	

Evidence	<form class="elementor-form" method="post" id="get_a_call_back" name="getacallback" aria-label="getacallback">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "form-field-country_code" "form-field-email" "form-field-mobile_number" "form-field-name" "form_id" "post_id" "queried_id" "referer_title"].
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbajajamc.dev.diginnovators.site%2Fwp-admin%2F
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="https://bajajamc.dev.diginnovators.site/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
Instances	5
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://bajajamc.dev.diginnovators.site/wp-login.php
Method	GET
Attack	
Evidence	frame-ancestors 'self';
Other Info	The directive(s): form-action is/are among the directives that do not fallback to default-src.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	frame-ancestors 'self';
Other Info	The directive(s): form-action is/are among the directives that do not fallback to default-src.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbajajamc.dev.diginnovators.site%2Fwp-admin%2F
Method	GET
Attack	
Evidence	frame-ancestors 'self';
Other Info	The directive(s): form-action is/are among the directives that do not fallback to default-src.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php
Method	POST
Attack	
Evidence	frame-ancestors 'self';
Other Info	The directive(s): form-action is/are among the directives that do not fallback to default-src.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	frame-ancestors 'self';
Other Info	The directive(s): form-action is/are among the directives that do not fallback to default-src.
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: 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://bajajamc.dev.diginnovators.site/wp-login.php
Method	GET
Attack	
Evidence	frame-ancestors 'self';
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://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	frame-ancestors 'self';
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://bajajamc.dev.diginnovators.site/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbajajamc.dev.diginnovators.site%2Fwp-admin%2F
Method	GET
Attack	
Evidence	frame-ancestors 'self';
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://bajajamc.dev.diginnovators.site/wp-login.php
Method	POST
Attack	
Evidence	frame-ancestors 'self';
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://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	frame-ancestors 'self';
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	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/

	https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: 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://bajajamc.dev.diginnovators.site/wp-login.php
Method	GET
Attack	
Evidence	frame-ancestors 'self';
Other Info	script-src includes unsafe-inline.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	frame-ancestors 'self';
Other Info	script-src includes unsafe-inline.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbajajamc.dev.diginnovators.site%2Fwp-admin%2F
Method	GET
Attack	
Evidence	frame-ancestors 'self';
Other Info	script-src includes unsafe-inline.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php
Method	POST
Attack	
Evidence	frame-ancestors 'self';
Other Info	script-src includes unsafe-inline.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	frame-ancestors 'self';
Other Info	script-src includes unsafe-inline.
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**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://bajajamc.dev.diginnovators.site/wp-login.php
Method	GET
Attack	
Evidence	frame-ancestors 'self';
Other Info	style-src includes unsafe-inline.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	frame-ancestors 'self';
Other Info	style-src includes unsafe-inline.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbajajamc.dev.diginnovators.site%2Fwp-admin%2F
Method	GET
Attack	
Evidence	frame-ancestors 'self';
Other Info	style-src includes unsafe-inline.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php
Method	POST
Attack	
Evidence	frame-ancestors 'self';
Other Info	style-src includes unsafe-inline.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	frame-ancestors 'self';
Other Info	style-src includes unsafe-inline.

Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

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

Other Info	
Instances	5
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	**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://bajajamc.dev.diginnovators.site/
Method	GET
Attack	
Evidence	<link rel='stylesheet' id='elementor-gf-rubik-css' href='https://fonts.googleapis.com/css?family=Rubik:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&#038;display=swap' media='all' />
Other Info	
URL	https://bajajamc.dev.diginnovators.site/glossary/
Method	GET
Attack	
Evidence	<link rel='stylesheet' id='elementor-gf-rubik-css' href='https://fonts.googleapis.com/css?family=Rubik:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&#038;display=swap' media='all' />
Other Info	
URL	https://bajajamc.dev.diginnovators.site/videos/
Method	GET
Attack	
Evidence	<link rel='stylesheet' id='elementor-gf-rubik-css' href='https://fonts.googleapis.com/css?family=Rubik:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&#038;display=swap' media='all' />
Other Info	
URL	https://bajajamc.dev.diginnovators.site/web-stories/
Method	GET
Attack	
Evidence	<link rel='stylesheet' id='elementor-gf-rubik-css' href='https://fonts.googleapis.com/css?family=Rubik:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&#038;display=swap' media='all' />

Other Info	
URL	https://bajajamc.dev.diginnovators.site/wp-content/uploads/wpo/wpo-plugins-tables-list.json
Method	GET
Attack	
Evidence	<link rel='stylesheet' id='elementor-gf-rubik-css' href='https://fonts.googleapis.com/css?family=Rubik:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&#038;display=swap' media='all' />
Other Info	
Instances	5
Solution	Provide a valid integrity attribute to the tag.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
CWE Id	345
WASC Id	15
Plugin Id	90003

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://bajajamc.dev.diginnovators.site/wp-login.php
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbajajamc.dev.diginnovators.site%2Fwp-admin%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	https://bajajamc.dev.diginnovators.site/wp-login.php
Method	POST
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	

URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
Instances	5
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://bajajamc.dev.diginnovators.site/web-story/key-habits-for-confident-investing-2/
Method	GET
Attack	
Evidence	<script async src="https://cdn.ampproject.org/v0.js"></script>
Other Info	
URL	https://bajajamc.dev.diginnovators.site/web-story/key-habits-for-confident-investing-2/
Method	GET
Attack	
Evidence	<script async custom-element="amp-story" src="https://cdn.ampproject.org/v0/amp-story-1.0.js"></script>
Other Info	
URL	https://bajajamc.dev.diginnovators.site/web-story/key-habits-for-confident-investing-2/
Method	GET
Attack	
Evidence	<script async custom-element="amp-video" src="https://cdn.ampproject.org/v0/amp-video-0.1.js"></script>
Other Info	
URL	https://bajajamc.dev.diginnovators.site/web-story/key-habits-for-confident-investing/
Method	GET
Attack	
Evidence	<script async src="https://cdn.ampproject.org/v0.js"></script>
Other Info	
URL	https://bajajamc.dev.diginnovators.site/web-story/key-habits-for-confident-investing/
Method	GET
Attack	
	<script async custom-element="amp-story" src="https://cdn.ampproject.org/v0/amp-story-

Evidence	1.0.js"></script>
Other Info	
Instances	5
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	**Secure Pages Include Mixed Content**
Description	The page includes mixed content, that is content accessed via HTTP instead of HTTPS.
URL	https://bajajamc.dev.diginnovators.site/
Method	GET
Attack	
Evidence	http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png
Other Info	tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png tag=img src=http://Long-term%20growth tag=img src=http://Long-term%20growth
URL	https://bajajamc.dev.diginnovators.site/glossary/
Method	GET
Attack	
Evidence	http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png
Other Info	tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png
URL	https://bajajamc.dev.diginnovators.site/videos/
Method	GET
Attack	
Evidence	http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png
Other Info	tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png
URL	https://bajajamc.dev.diginnovators.site/web-stories/
Method	GET
Attack	
Evidence	http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png
Other Info	tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png
URL	https://bajajamc.dev.diginnovators.site/wp-content/uploads/wpo/wpo-plugins-tables-list.json
Method	GET

Attack	
Evidence	http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png
Other Info	tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png tag=img src=http://bajajamc.dev.diginnovators.site/wp-content/uploads/2025/11/Avatar-on-header.png
Instances	5
Solution	A page that is available over SSL/TLS must be comprised completely of content which is transmitted over SSL/TLS. The page must not contain any content that is transmitted over unencrypted HTTP. This includes content from third party sites.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
CWE Id	311
WASC Id	4
Plugin Id	10040

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://bajajamc.dev.diginnovators.site/videos/
Method	GET
Attack	
Evidence	1768670208
Other Info	1768670208, which evaluates to: 2026-01-17 22:46:48.
URL	https://bajajamc.dev.diginnovators.site/videos/
Method	GET
Attack	
Evidence	1768670214
Other Info	1768670214, which evaluates to: 2026-01-17 22:46:54.
URL	https://bajajamc.dev.diginnovators.site/videos/
Method	GET
Attack	
Evidence	1768670215
Other Info	1768670215, which evaluates to: 2026-01-17 22:46:55.
URL	https://bajajamc.dev.diginnovators.site/videos/
Method	GET
Attack	
Evidence	1768670217
Other Info	1768670217, which evaluates to: 2026-01-17 22:46:57.
URL	https://bajajamc.dev.diginnovators.site/videos/
Method	GET

Attack	
Evidence	1768714546
Other Info	1768714546, which evaluates to: 2026-01-18 11:05:46.
Instances	5
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

Informational	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://bajajamc.dev.diginnovators.site/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fbajajamc.dev.diginnovators.site%2Fvideos%2F
Method	GET
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	1
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	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://bajajamc.dev.diginnovators.site/wp-admin/js/user-profile.min.js?ver=6.9
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in likely comment: "//www.w3.org/2000/svg" fill="#3c434a" stroke="#3c434a" stroke-width="0.5"><path d="M12 5L19 15H16V19H8V15H5L12 5Z"/><rect x="8" ", see evidence field for the suspicious comment /snippet.
URL	https://bajajamc.dev.diginnovators.site/wp-content/plugins/elementor-pro/assets/js/elements-handlers.min.js?ver=3.33.2

Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//www.w3.org/2000/svg","svg"),IconsManager.symbolsContainer.setAttributeNS(null,"style","display:none;"),IconsManager.symbolsCo", see evidence field for the suspicious comment/snippet.
URL	https://bajajamc.dev.diginnovators.site/wp-content/plugins/elementor-pro/assets/lib/smartmenus/jquery.smartmenus.min.js?ver=1.2.1
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//vadikom.com; Licensed MIT */!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):"object"==typeof module&&"", see evidence field for the suspicious comment/snippet.
URL	https://bajajamc.dev.diginnovators.site/wp-content/plugins/elementor/assets/js/frontend-modules.min.js?ver=3.33.3
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//github.com/zloirock/core-js/blob/v3.43.0/LICENSE",source:"https://github.com/zloirock/core-js"})},1851:(t,e,r)=>{"use strict";", see evidence field for the suspicious comment/snippet.
URL	https://bajajamc.dev.diginnovators.site/wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.33.3
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//player.vimeo.com/api/player.js"}getURLRegex(){return/^(?:https?:\/\/)?(?:www|player\.)?(?:vimeo\.com\/)?(?:video\/|external\/)", see evidence field for the suspicious comment/snippet.
URL	https://bajajamc.dev.diginnovators.site/wp-content/themes/hello-theme-child-master/assets/js/charts.js?ver=1.0
Method	GET
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in likely comment: "//www.gstatic.com/charts/%{version}/loader.js"),debug:l("https://www.gstatic.com/charts/debug/%{version}/js/jsapi_debug_%{packag", see evidence field for the suspicious comment/snippet.
URL	https://bajajamc.dev.diginnovators.site/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//,Bt={},_t={},zt="*/".concat("*"),Xt=C.createElement("a");function Ut(o){return function(e,t){"string"!=typeof e&&(t=e,e="*");v", see evidence field for the suspicious comment/snippet.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php
Method	GET

Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in likely comment: "//bajajamc.dev.diginnovators.site/wp-admin/js/password-strength-meter.min.js?ver=6.9" id="password-strength-meter-js"></script>", see evidence field for the suspicious comment/snippet.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//# sourceURL=user-profile-js-extra", see evidence field for the suspicious comment/snippet.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbajajamc.dev.diginnovators.site%2Fwp-admin%2F
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in likely comment: "//bajajamc.dev.diginnovators.site/wp-admin/js/password-strength-meter.min.js?ver=6.9" id="password-strength-meter-js"></script>", see evidence field for the suspicious comment/snippet.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbajajamc.dev.diginnovators.site%2Fwp-admin%2F
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//# sourceURL=user-profile-js-extra", see evidence field for the suspicious comment/snippet.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in likely comment: "//bajajamc.dev.diginnovators.site/wp-admin/js/password-strength-meter.min.js?ver=6.9" id="password-strength-meter-js"></script>", see evidence field for the suspicious comment/snippet.
URL	https://bajajamc.dev.diginnovators.site/wp-login.php
Method	POST
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//# sourceURL=user-profile-js-extra", see evidence field for the suspicious comment/snippet.
Instances	13
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13

Plugin Id	10027

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://bajajamc.dev.diginnovators.site/
Method	GET
Attack	
Evidence	<a class="e-n-menu-title-container e-focus e-link" href="#" aria-current="page"> <span class="e-n-menu-title-text"> All Funds </span> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://bajajamc.dev.diginnovators.site/glossary/
Method	GET
Attack	
Evidence	<a class="e-n-menu-title-container e-focus e-link" href="#" aria-current="page"> <span class="e-n-menu-title-text"> All Funds </span> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://bajajamc.dev.diginnovators.site/videos/
Method	GET
Attack	
Evidence	<a class="e-n-menu-title-container e-focus e-link" href="#" aria-current="page"> <span class="e-n-menu-title-text"> All Funds </span> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://bajajamc.dev.diginnovators.site/web-stories/
Method	GET
Attack	
Evidence	<a class="e-n-menu-title-container e-focus e-link" href="#" aria-current="page"> <span class="e-n-menu-title-text"> All Funds </span> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://bajajamc.dev.diginnovators.site/wp-content/uploads/wpo/wpo-plugins-tables-list.json
Method	GET
Attack	
Evidence	<a class="e-n-menu-title-container e-focus e-link" href="#" aria-current="page"> <span class="e-n-menu-title-text"> All Funds </span> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Instances	5
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	Re-examine Cache-control Directives
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://bajajamc.dev.diginnovators.site/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bajajamc.dev.diginnovators.site/videos/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bajajamc.dev.diginnovators.site/wp-json/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bajajamc.dev.diginnovators.site/wp-sitemap-index.xsl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bajajamc.dev.diginnovators.site/wp-sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	5
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	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://bajajamc.dev.diginnovators.site/wp-login.php
Method	GET
Attack	
Evidence	wordpress_test_cookie
Other Info	cookie:wordpress_test_cookie
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	wordpress_test_cookie
Other Info	cookie:wordpress_test_cookie
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbajajamc.dev.diginnovators.site%2Fwp-admin%2F
Method	GET
Attack	
Evidence	wordpress_test_cookie
Other Info	cookie:wordpress_test_cookie
URL	https://bajajamc.dev.diginnovators.site/wp-login.php
Method	POST
Attack	
Evidence	wordpress_test_cookie
Other Info	cookie:wordpress_test_cookie
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	wordpress_test_cookie
Other Info	cookie:wordpress_test_cookie
Instances	5
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/
CWE Id	
WASC Id	
Plugin Id	10112

Informational	User Controllable HTML Element Attribute (Potential XSS)

Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/?e-filter-ccaa784-glossary-type=mutual-fund&e-filter-e0a7636-category=wealth-creation
Method	GET
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://bajajamc.dev.diginnovators.site/knowledge-centre/?e-filter-ccaa784-glossary-type=mutual-fund&e-filter-e0a7636-category=wealth-creation appears to include user input in: a(n) [button] tag [data-filter] attribute The user input found was: e-filter-ccaa784-glossary-type=mutual-fund The user-controlled value was: mutual-funds-101
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/?e-filter-ccaa784-glossary-type=mutual-fund&e-filter-e0a7636-category=wealth-creation
Method	GET
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://bajajamc.dev.diginnovators.site/knowledge-centre/?e-filter-ccaa784-glossary-type=mutual-fund&e-filter-e0a7636-category=wealth-creation appears to include user input in: a(n) [button] tag [data-filter] attribute The user input found was: e-filter-e0a7636-category=wealth-creation The user-controlled value was: wealth-creation
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	GET
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://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword appears to include user input in: a(n) [form] tag [name] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbajajamc.dev.diginnovators.site%2Fwp-admin%2F
Method	GET
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://bajajamc.dev.diginnovators.site/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbajajamc.dev.diginnovators.site%2Fwp-admin%2F appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://bajajamc.dev.diginnovators.site/wp-admin/ The user-controlled value was: https://bajajamc.dev.diginnovators.site/wp-admin/css/forms.min.css?ver=6.9
URL	https://bajajamc.dev.diginnovators.site/contact-us/
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: https://bajajamc.dev.diginnovators.site/contact-us/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/contact-us/
Method	POST
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://bajajamc.dev.diginnovators.site/contact-us/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/contact-us/
Method	POST
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://bajajamc.dev.diginnovators.site/contact-us/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/contact-us/
Method	POST
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://bajajamc.dev.diginnovators.site/contact-us/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/contact-us/embed/
Method	POST
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://bajajamc.dev.diginnovators.site/contact-us/embed/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/contact-us/embed/
Method	POST
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://bajajamc.dev.diginnovators.site/contact-us/embed/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/contact-us/embed/
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: https://bajajamc.dev.diginnovators.site/contact-us/embed/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/contact-us/embed/
Method	POST
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://bajajamc.dev.diginnovators.site/contact-us/embed/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/fund-listing/
Method	POST
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://bajajamc.dev.diginnovators.site/fund-listing/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/fund-listing/
Method	POST
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://bajajamc.dev.diginnovators.site/fund-listing/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/fund-listing/
Method	POST
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://bajajamc.dev.diginnovators.site/fund-listing/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/fund-listing/
Method	POST
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://bajajamc.dev.diginnovators.site/fund-listing/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-2/
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-2/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields [country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-2/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-2/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-2/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-2/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-2/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-2/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-3/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-3/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields [country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-3/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-3/ appears to include user

Info	input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-3/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-3/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-3/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-3/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-4/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-4/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-4/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-4/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-4/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-4/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609

URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-4/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-4/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-5/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-5/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-5/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-5/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-5/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-5/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-5/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market-5/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market/

Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market/
Method	POST
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://bajajamc.dev.diginnovators.site/glossary/where-the-opportunities-are-in-the-current-market/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-10/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-10/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-10/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-10/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-10/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-10/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-10/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-10/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-2/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-2/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-2/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-2/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-2/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-2/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-2/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-2/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-3/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-3/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-3/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-3/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-3/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-3/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-3/
Method	POST
Attack	
Evidence	
	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://bajajamc.dev.diginnovators.

Other Info	site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-3/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-4/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-4/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields [country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-4/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-4/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-4/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-4/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-4/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-4/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-5/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.

Info	site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-5/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields [country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-5/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-5/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-5/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-5/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-5/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-5/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-6/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-6/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields [country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-6/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.

Info	site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-6/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-6/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-6/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-6/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-6/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-7/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-7/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-7/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-7/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-7/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.

Info	site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-7/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-7/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-7/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-8/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-8/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-8/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-8/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-8/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-8/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-8/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.

Info	site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-8/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-9/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-9/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-9/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-9/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-9/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-9/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-9/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments-9/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.

Info	site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields [country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/lorem-ispam-risks-in-mutual-fund-investments/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/why-should-you-alter-your-investment-strategy-based-on-your-changing-financial-goals/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/why-should-you-alter-your-investment-strategy-based-on-your-changing-financial-goals/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/why-should-you-alter-your-investment-strategy-based-on-your-changing-financial-goals/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.site/knowledge-centre/why-should-you-alter-your-investment-strategy-based-on-your-

Info	changing-financial-goals/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/why-should-you-alter-your-investment-strategy-based-on-your-changing-financial-goals/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/why-should-you-alter-your-investment-strategy-based-on-your-changing-financial-goals/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/knowledge-centre/why-should-you-alter-your-investment-strategy-based-on-your-changing-financial-goals/
Method	POST
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://bajajamc.dev.diginnovators.site/knowledge-centre/why-should-you-alter-your-investment-strategy-based-on-your-changing-financial-goals/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/lorem-ispam-risks-in-mutual-fund-investments/
Method	POST
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://bajajamc.dev.diginnovators.site/lorem-ispam-risks-in-mutual-fund-investments/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/lorem-ispam-risks-in-mutual-fund-investments/
Method	POST
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://bajajamc.dev.diginnovators.site/lorem-ispam-risks-in-mutual-fund-investments/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/lorem-ispam-risks-in-mutual-fund-investments/
Method	POST
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://bajajamc.dev.diginnovators.site/lorem-ispam-risks-in-mutual-fund-investments/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/lorem-ispam-risks-in-mutual-fund-investments/
Method	POST

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://bajajamc.dev.diginnovators.site/lorem-ispam-risks-in-mutual-fund-investments/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-2/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-2/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-2/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-2/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-2/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-2/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-2/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-2/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-3/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-3/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-3/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-3/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-3/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-3/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-3/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds-3/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds/
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: https://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/how-bajaj-finserv-carpet-bombed-its-way-to-2-2b-in-mutual-funds/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-2/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-2/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-2/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-2/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-2/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-

Info	first-year-2/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-2/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-2/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-3/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-3/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-3/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-3/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-3/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-3/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-3/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year-3/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16

URL	https://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year/
Method	POST
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://bajajamc.dev.diginnovators.site/media-centre/the-bajaj-name-eased-our-way-ganesh-mohan-ceo-on-bajaj-finserv-mfs-first-year/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/
Method	POST

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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/cagr-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/cagr-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/cagr-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/cagr-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/cagr-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/cagr-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/cagr-calculator/

Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/cagr-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/car-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/car-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/car-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/car-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/car-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/car-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/car-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/car-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/child-education-calculator/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.

Info	site/mutual-fund-calculators/child-education-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/child-education-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/child-education-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/child-education-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/child-education-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/child-education-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/child-education-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/compounding-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/compounding-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/compounding-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/compounding-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/compounding-calculator/
Method	POST

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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/compounding-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/compounding-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/compounding-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/dream-home-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/dream-home-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/dream-home-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/dream-home-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/dream-home-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/dream-home-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/dream-home-calculator/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/dream-home-calculator/ appears to include user input in: a(n)

Info	[svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/elss-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/elss-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/elss-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/elss-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/elss-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/elss-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/elss-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/elss-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/epf-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/epf-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/epf-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/epf-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/epf-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/epf-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/epf-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/epf-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/income-tax-calculator-2/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/income-tax-calculator-2/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/income-tax-calculator-2/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/income-tax-calculator-2/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/income-tax-calculator-2/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/income-tax-calculator-2/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/income-tax-calculator-2/

Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/income-tax-calculator-2/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/index-fund-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/index-fund-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/index-fund-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/index-fund-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/index-fund-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/index-fund-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/index-fund-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/index-fund-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/investment-calculator/
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/investment-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/investment-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/investment-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/investment-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/investment-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/investment-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/investment-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/lumpsum-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/lumpsum-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/lumpsum-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/lumpsum-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/lumpsum-calculator/

Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/lumpsum-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/lumpsum-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/lumpsum-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/mutual-fund-returns-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/mutual-fund-returns-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/mutual-fund-returns-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/mutual-fund-returns-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/mutual-fund-returns-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/mutual-fund-returns-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/mutual-fund-returns-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/mutual-fund-returns-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/ppf-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/ppf-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/ppf-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/ppf-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/ppf-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/ppf-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/ppf-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/ppf-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/retirement-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/retirement-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/retirement-calculator/

Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/retirement-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/retirement-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/retirement-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/retirement-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/retirement-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/simple-interst-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/simple-interst-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/simple-interst-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/simple-interst-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/simple-interst-calculator/
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/simple-interst-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/simple-interst-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/simple-interst-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-step-up-sip-calculator/
Method	POST

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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-step-up-sip-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-step-up-sip-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-step-up-sip-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-step-up-sip-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-step-up-sip-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-step-up-sip-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/sip-step-up-sip-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/stp-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/stp-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/stp-calculator/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/stp-calculator/ appears to include user input in: a(n) [div] tag

Info	[data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/stp-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/stp-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/stp-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/stp-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/swp-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/swp-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/swp-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/swp-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/swp-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/swp-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/swp-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/swp-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/wealth-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/wealth-calculator/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/wealth-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/wealth-calculator/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/wealth-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/wealth-calculator/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/mutual-fund-calculators/wealth-calculator/
Method	POST
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://bajajamc.dev.diginnovators.site/mutual-fund-calculators/wealth-calculator/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/sip/
Method	POST
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://bajajamc.dev.diginnovators.site/sip/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/sip/

Method	POST
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://bajajamc.dev.diginnovators.site/sip/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/sip/
Method	POST
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://bajajamc.dev.diginnovators.site/sip/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/sip/
Method	POST
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://bajajamc.dev.diginnovators.site/sip/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/sip/embed/
Method	POST
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://bajajamc.dev.diginnovators.site/sip/embed/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/sip/embed/
Method	POST
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://bajajamc.dev.diginnovators.site/sip/embed/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/sip/embed/
Method	POST
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://bajajamc.dev.diginnovators.site/sip/embed/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/sip/embed/
Method	POST

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://bajajamc.dev.diginnovators.site/sip/embed/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-10/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-10/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-10/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-10/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-10/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-10/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-10/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-10/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-11/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.

Info	site/where-the-opportunities-are-in-the-current-market-11/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code] =+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-11/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-11/ appears to include user input in: a (n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-11/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-11/ appears to include user input in: a (n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-11/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-11/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-12/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-12/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code] =+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-12/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-12/ appears to include user input in: a (n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-12/
Method	POST

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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-12/ appears to include user input in: a (n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-12/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-12/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-13/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-13/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code] =+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-13/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-13/ appears to include user input in: a (n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-13/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-13/ appears to include user input in: a (n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-13/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-13/ appears to include user input in: a

Info	(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-14/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-14/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-14/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-14/ appears to include user input in: a (n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-14/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-14/ appears to include user input in: a (n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-14/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-14/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-15/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-15/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-15/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-15/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-15/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-15/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-15/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-15/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-16/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-16/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-16/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-16/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-16/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-16/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609

URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-16/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-16/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-17/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-17/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code] =+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-17/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-17/ appears to include user input in: a (n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-17/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-17/ appears to include user input in: a (n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-17/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-17/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-18/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-18/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-18/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-18/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-18/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-18/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-18/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-18/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-19/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-19/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-19/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-19/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-19/

Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-19/ appears to include user input in: a (n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-19/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-19/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-2/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-2/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code] =+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-2/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-2/ appears to include user input in: a (n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-2/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-2/ appears to include user input in: a (n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-2/
Method	POST
Attack	
Evidence	
	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://bajajamc.dev.diginnovators.

Other Info	site/where-the-opportunities-are-in-the-current-market-2/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-20/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-20/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code] =+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-20/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-20/ appears to include user input in: a (n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-20/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-20/ appears to include user input in: a (n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-20/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-20/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-21/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-21/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code] =+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-21/
Method	POST

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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-21/ appears to include user input in: a (n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-21/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-21/ appears to include user input in: a (n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-21/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-21/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-3/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-3/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code] =+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-3/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-3/ appears to include user input in: a (n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-3/
Method	POST
Attack	
Evidence	
Other	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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-3/ appears to include user input in: a

Info	(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-3/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-3/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-4/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-4/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code] =+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-4/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-4/ appears to include user input in: a (n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-4/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-4/ appears to include user input in: a (n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-4/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-4/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-5/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-5/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code] =+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-5/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-5/ appears to include user input in: a (n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-5/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-5/ appears to include user input in: a (n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-5/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-5/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-6/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-6/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code] =+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-6/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-6/ appears to include user input in: a (n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77

URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-6/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-6/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-6/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-6/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-7/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-7/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-7/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-7/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-7/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-7/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-7/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-7/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-8/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-8/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code] =+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-8/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-8/ appears to include user input in: a (n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-8/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-8/ appears to include user input in: a (n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-8/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-8/ appears to include user input in: a (n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-9/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-9/ appears to include user input in: a (n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code] =+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-9/

Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-9/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-9/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-9/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-9/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market-9/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market/ appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: form_fields[country_code]=+91 The user-controlled value was: +91
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=92e3a77 The user-controlled value was: 92e3a77
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market/
Method	POST
Attack	
Evidence	
	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://bajajamc.dev.diginnovators.

Other Info	site/where-the-opportunities-are-in-the-current-market/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=4609 The user-controlled value was: 4609
URL	https://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market/
Method	POST
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://bajajamc.dev.diginnovators.site/where-the-opportunities-are-in-the-current-market/ appears to include user input in: a(n) [svg] tag [width] attribute The user input found was: queried_id=16 The user-controlled value was: 16
URL	https://bajajamc.dev.diginnovators.site/wp-login.php
Method	POST
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://bajajamc.dev.diginnovators.site/wp-login.php appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://bajajamc.dev.diginnovators.site/wp-admin/ The user-controlled value was: https://bajajamc.dev.diginnovators.site/wp-admin/css/forms.min.css?ver=6.9
URL	https://bajajamc.dev.diginnovators.site/wp-login.php
Method	POST
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://bajajamc.dev.diginnovators.site/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: rememberme=forever The user-controlled value was: forever
URL	https://bajajamc.dev.diginnovators.site/wp-login.php
Method	POST
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://bajajamc.dev.diginnovators.site/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: wp-submit=Log In The user-controlled value was: log in
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	POST
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://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword appears to include user input in: a(n) [form] tag [name] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	POST
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://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword appears to include user input in: a(n) [input] tag [value] attribute The user input found was: user_login=ZAP The user-controlled value was: zap
URL	https://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword
Method	POST
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://bajajamc.dev.diginnovators.site/wp-login.php?action=lostpassword appears to include user input in: a(n) [input] tag [value] attribute The user input found was: wp-submit=Get New Password The user-controlled value was: get new password
Instances	290
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