VirtuesTech Security Scan Report

Sites: http://virtuestech.com https://virtuestech.com

Generated on Wed, 9 Apr 2025 16:27:14

Summary of Alerts

RISK LEVEL	NUMBER OF ALERTS
High	0
Medium	8
Low	7
Informational	7
False Positives:	0

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Alerts

NAME	RISK LEVEL	NUMBER OF INSTANCES
Absence of Anti-CSRF Tokens	Medium	72
CSP: Failure to Define Directive with No Fallback	Medium	233
CSP: Wildcard Directive	Medium	233
CSP: script-src unsafe-inline	Medium	233
CSP: style-src unsafe-inline	Medium	233
Content Security Policy (CSP) Header Not Set	Medium	2
Missing Anti-clickjacking Header	Medium	148
Vulnerable JS Library	Medium	1

Cookie No HttpOnly Flag	Low	5
Cookie without SameSite Attribute	Low	5
Cross-Domain JavaScript Source File Inclusion	Low	115
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	435
Strict-Transport-Security Header Not Set	Low	720
Timestamp Disclosure - Unix	Low	568
X-Content-Type-Options Header Missing	Low	529
Charset Mismatch	Informational	59
Information Disclosure - Suspicious Comments	Informational	43
Modern Web Application	Informational	112
Re-examine Cache-control Directives	Informational	313
Retrieved from Cache	Informational	305
Session Management Response Identified	Informational	6
User Controllable HTML Element Attribute (Potential XSS)	Informational	522

Alert Detail

MEDIUM	ABSENCE OF ANTI-CSRF TOKENS

Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://virtuestech.com
Method	GET
Parameter	
Attack	
Evidence	<form action="/#wpcf7-f15142-p22906-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/
Method	GET
Parameter	
Attack	
Evidence	<form action="/#wpcf7-f15142-p22906-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/ai-driven-test-automation-2/

Method	GET
Parameter	
Attack	
Evidence	<form action="/ai-driven-test-automation-2/#wpcf7-f15142-p20009-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	
Attack	
Evidence	<form action="/atlas/#wpcf7-f15142-p21974-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/contact/
Method	GET
Parameter	
Attack	
Evidence	<form action="/contact/#wpcf7-f15142-p256-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	
Attack	
Evidence	<form action="https://virtuestech.com/wp-comments-post.php" method="post" id="commentform" class="comment-form" novalidate>

Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "author" "comment_parent" "comment_post_ID" "email" "submit" "url" "wp-comment-cookies-consent"].
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/accessibility-usability-testing/#wpcf7-f15142-p22566-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/advisory-and-transformation/#wpcf7-f15142-p19466-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/agile-and-devops-testing/#wpcf7-f15142-p22591-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET

Parameter	
Attack	
Evidence	<form action="/services/ai-driven-test-automation/#wpcf7-f15142-p19359-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/api-security-testing/#wpcf7-f15142-p20738-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/api-testing-services/#wpcf7-f15142-p14382-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/business-experience-validation/#wpcf7-f15142-p20587-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>

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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/cloud-native-application-testing/#wpcf7-f15142-p22576-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/cloud-security-testing/#wpcf7-f15142-p20754-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/compliance-and-security-audits/#wpcf7-f15142-p22685-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/

Method	GET
Parameter	
Attack	
Evidence	<form action="/services/comprehensive-test-automation-framework/#wpcf7-f15142-p22561-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/continuous-quality-engineering/#wpcf7-f15142-p19537-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/cyber-resilience-testing/#wpcf7-f15142-p22695-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/data-driven-testing/#wpcf7-f15142-p22571-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>

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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/devsecops-integration/#wpcf7-f15142-p22680-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/iot-and-embedded-systems-testing/#wpcf7-f15142-p22581-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/iot-security-testing/#wpcf7-f15142-p22675-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/managed-soc-services/

Method	GET
Parameter	
Attack	
Evidence	<form action="/services/managed-soc-services/#wpcf7-f15142-p20790-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/manual-testing-services/#wpcf7-f15142-p13749-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/mobile-security-testing/#wpcf7-f15142-p22700-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/penetration-testing/#wpcf7-f15142-p20670-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>

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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/performance-Engineering-Monitoring/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/performance-Engineering-Monitoring/#wpcf7-f15142-p14364-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/performance-engineering-monitoring/#wpcf7-f15142-p14364-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/secure-code-validation/#wpcf7-f15142-p22690-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/

Method	GET
Parameter	
Attack	
Evidence	<form action="/services/shift-left-and-shift-right-testing/#wpcf7-f15142-p22586-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/test-center-of-excellence/#wpcf7-f15142-p20606-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/vulnerability-assessment/#wpcf7-f15142-p20732-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	
Attack	
Evidence	<form action="/services/zero-trust-network-assessments/#wpcf7-f15142-p22708-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init">>

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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	
Attack	
Evidence	<form action="https://virtuestech.com/wp-comments-post.php" method="post" id="commentform" class="comment-form" novalidate>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "author" "comment_parent" "comment_post_ID" "email" "submit" "url" "wp-comment-cookies-consent"].
URL	https://virtuestech.com/wp-login.php
Method	GET
Parameter	
Attack	
Evidence	<form name="loginform" id="loginform" action="https://virtuestech.com/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"].
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET
Parameter	
Attack	
Evidence	<form name="lostpasswordform" id="lostpasswordform" action="https://virtuestech.com/wp-login.php?action=lostpassword" 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" "user_login" "wp-submit"].
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	
Attack	

Evidence	<form name="loginform" id="loginform" action="https://virtuestech.com/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"].
URL	https://virtuestech.com/
Method	POST
Parameter	
Attack	
Evidence	<form action="/#wpcf7-f15142-p22906-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	
Attack	
Evidence	<form action="/ai-driven-test-automation-2/#wpcf7-f15142-p20009-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	
Attack	
Evidence	<form action="/atlas/#wpcf7-f15142-p21974-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].

URL	https://virtuestech.com/contact/
Method	POST
Parameter	
Attack	
Evidence	<form action="/contact/#wpcf7-f15142-p256-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/accessibility-usability-testing/#wpcf7-f15142-p22566-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/advisory-and-transformation/#wpcf7-f15142-p19466-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/agile-and-devops-testing/#wpcf7-f15142-p22591-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>

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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/ai-driven-test-automation/#wpcf7-f15142-p19359-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/api-security-testing/#wpcf7-f15142-p20738-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/api-testing-services/#wpcf7-f15142-p14382-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/business-experience-validation/

Method	POST
Parameter	
Attack	
Evidence	<form action="/services/business-experience-validation/#wpcf7-f15142-p20587-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/cloud-native-application-testing/#wpcf7-f15142-p22576-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/cloud-security-testing/#wpcf7-f15142-p20754-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/compliance-and-security-audits/#wpcf7-f15142-p22685-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>

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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/comprehensive-test-automation-framework/#wpcf7-f15142-p22561-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/continuous-quality-engineering/#wpcf7-f15142-p19537-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/cyber-resilience-testing/#wpcf7-f15142-p22695-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/data-driven-testing/

Method	POST
Parameter	
Attack	
Evidence	<form action="/services/data-driven-testing/#wpcf7-f15142-p22571-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/devsecops-integration/#wpcf7-f15142-p22680-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/iot-and-embedded-systems-testing/#wpcf7-f15142-p22581-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/iot-security-testing/#wpcf7-f15142-p22675-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>

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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/managed-soc-services/#wpcf7-f15142-p20790-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/manual-testing-services/#wpcf7-f15142-p13749-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/mobile-security-testing/#wpcf7-f15142-p22700-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/penetration-testing/

Method	POST
Parameter	
Attack	
Evidence	<form action="/services/penetration-testing/#wpcf7-f15142-p20670-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/performance-Engineering-Monitoring/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/performance-Engineering-Monitoring/#wpcf7-f15142-p14364-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/performance-engineering-monitoring/#wpcf7-f15142-p14364-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/secure-code-validation/#wpcf7-f15142-p22690-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>

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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/shift-left-and-shift-right-testing/#wpcf7-f15142-p22586-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/test-center-of-excellence/#wpcf7-f15142-p20606-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	
Attack	
Evidence	<form action="/services/vulnerability-assessment/#wpcf7-f15142-p20732-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">>
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/services/zero-trust-network-assessments/

Method	POST
Parameter	
Attack	
Evidence	<form action="/services/zero-trust-network-assessments/#wpcf7-f15142-p22708-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">
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: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "email-873" "tel-969" "text-192" "text-438"].
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	
Attack	
Evidence	<form name="loginform" id="loginform" action="https://virtuestech.com/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"].
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	
Attack	
Evidence	<form name="lostpasswordform" id="lostpasswordform" action="https://virtuestech.com/wp-login.php?action=lostpassword" 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" "user_login" "wp-submit"].
Instances	72

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://virtuestech.com
Method	GET
Parameter	content-security-policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

URL	https://virtuestech.com/?p=1025
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=1039
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=1050
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=1078
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=13377
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=13410
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=13420
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=13428
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=13434
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=13610
Method	GET
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=13621
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=13645
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=13749
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=14364
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=14382
Method	GET
Parameter	Content-Security-Policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=15119
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=1522
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=1545
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=188
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=18967
Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=19359
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=19466
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=19537
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=20009
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=20339

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=20343
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=20365
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=20587
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=20606
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

URL	https://virtuestech.com/?p=20670
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=20732
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=20738
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=20754
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=20790
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=21232
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=21263
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=21974
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22176
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22561
Method	GET
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22566
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22571
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22576
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22581
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22586
Method	GET
Parameter	content-security-policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22591
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22675
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22680
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22685
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22690
Method	GET

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22695
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22700
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=22708
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=256
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=271

Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=3500
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=439
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=474
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/?p=5664
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

URL	https://virtuestech.com/?page_id=20760
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/about/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/about/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/advisorytransformation
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/ai-driven-test-automation-2/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/ai-driven-test-automation/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/atlas/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/blogs/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/blogs/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/blogs/page/2/?ajaxify=1
Method	GET
Parameter	Content-Security-Policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/careers/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/careers/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/category/quality-engineering/
Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/category/uncategorized/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/contact
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/contact/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/contact/embed/

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/continuous-quality-engineering
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/cybersecurity-services/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/industries/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/industries/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/insights/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/accessibility-usability-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/advisory-and-transformation/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/agile-and-devops-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	Content-Security-Policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/ai-driven-test-automation/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/api-security-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/api-testing-services
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/api-testing-services/
Method	GET

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/api-testing-services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/business-experience-validation/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/cloud-native-application-testing/embed/

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/cloud-security-testing
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/cloud-security-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

URL	https://virtuestech.com/services/compliance-and-security-audits/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/continuous-quality-engineering
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/continuous-quality-engineering/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/cyber-resilience-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/data-driven-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/devsecops-integration/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/embed/
Method	GET
Parameter	Content-Security-Policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/iot-security-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/managed-soc-services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/manual-testing-services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/mobile-security-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/penetration-testing/embed/

Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/performance-engineering-monitoring/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/performance-testing-services
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

URL	https://virtuestech.com/services/secure-code-validation/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/security-audits-and-compliance
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/test-center-of-excellence/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/vulnerability-assessment/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/zero-trust-network-assessments/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/sitemap.xml
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	content-security-policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/embed/
Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/wp-admin/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/wp-admin/admin-ajax.php
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/wp-login.php
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/contact/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/accessibility-usability-testing/

Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	Content-Security-Policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	content-security-policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/wp-comments-post.php
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://virtuestech.com/wp-login.php?action=lostpassword

Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
Instances	233
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	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://virtuestech.com
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/
Method	GET

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	content-security-policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=1025
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=1039
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=1050
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=1078
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=13377
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=13410
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=13420
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=13428
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=13434
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=13610
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=13621
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=13645
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=13749
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=14364
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=14382
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=15119
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=1522
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=1545
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=188
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=18967
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=19359
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=19466
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=19537
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=20009
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=20339
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=20343
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=20365
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=20587
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=20606
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=20670
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=20732
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=20738
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=20754
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=20790
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=21232
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=21263
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=21974
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22176
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22561
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22566
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22571
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22576
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22581
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22586
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22591
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22675
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22680
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22685
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22690
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22695
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22700
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=22708
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=256
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=271
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=3500
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=439
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=474
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?p=5664
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/?page_id=20760
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/about/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/about/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/advisorytransformation
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/ai-driven-test-automation-2/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/ai-driven-test-automation/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/atlas/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/best-practices-for-effective-software-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/blogs/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/blogs/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/blogs/page/2/?ajaxify=1
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/careers/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/careers/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/category/uncategorized/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/contact
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/contact/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/contact/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/continuous-quality-engineering
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/cybersecurity-services/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/industries/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/industries/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/insights/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/accessibility-usability-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/advisory-and-transformation/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/agile-and-devops-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/ai-driven-test-automation/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/api-security-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/api-testing-services
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/api-testing-services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/business-experience-validation/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/cloud-native-application-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/cloud-security-testing
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/cloud-security-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/compliance-and-security-audits/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/continuous-quality-engineering
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/continuous-quality-engineering/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/cyber-resilience-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/data-driven-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/devsecops-integration/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/iot-security-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/managed-soc-services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/manual-testing-services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/mobile-security-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/penetration-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/performance-engineering-monitoring/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/performance-testing-services
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/secure-code-validation/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/security-audits-and-compliance
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/test-center-of-excellence/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/vulnerability-assessment/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/zero-trust-network-assessments/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/sitemap.xml
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/why-do-the-mobile-manual-test/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/wp-admin/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/wp-admin/admin-ajax.php
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/wp-login.php
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/contact/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/wp-comments-post.php
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
Instances	233
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CWE Id	693
WASC Id	15
Plugin Id	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://virtuestech.com
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.

URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=1025
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=1039
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=1050
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=1078
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13377
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13410
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13420
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13428
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13434
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13610
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13621
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13645
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13749
Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=14364
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=14382
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=15119
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=1522
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=1545

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=188
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=18967
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=19359
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=19466
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.

URL	https://virtuestech.com/?p=19537
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20009
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20339
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20343
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20365
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20587
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20606
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20670
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20732
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20738
Method	GET
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20754
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20790
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=21232
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=21263
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=21974
Method	GET

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22176
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22561
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22566
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22571
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22576

Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22581
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22586
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22591
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22675
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.

URL	https://virtuestech.com/?p=22680
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22685
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22690
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22695
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22700
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22708
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=256
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=271
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=3500
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=439
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=474
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?p=5664
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/?page_id=20760
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/about/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/about/embed/
Method	GET
Parameter	content-security-policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/advisorytransformation
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/ai-driven-test-automation-2/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/ai-driven-test-automation/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/atlas/

Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/atlas/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.

URL	https://virtuestech.com/blogs/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/blogs/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/blogs/page/2/?ajaxify=1
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/careers/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/careers/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/category/uncategorized/
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/contact
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/contact/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/contact/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/continuous-quality-engineering
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/cybersecurity-services/
Method	GET
Parameter	Content-Security-Policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/embed/
Method	GET

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/industries/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/industries/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/insights/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/

Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/accessibility-usability-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/advisory-and-transformation/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.

URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/agile-and-devops-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/ai-driven-test-automation/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-security-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-testing-services
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-testing-services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/business-experience-validation/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-native-application-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-security-testing
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-security-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/compliance-and-security-audits/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/embed/

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/continuous-quality-engineering
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/continuous-quality-engineering/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.

URL	https://virtuestech.com/services/cyber-resilience-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/data-driven-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/devsecops-integration/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/iot-security-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/managed-soc-services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/manual-testing-services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	Content-Security-Policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/mobile-security-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/penetration-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/performance-engineering-monitoring/embed/
Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/performance-testing-services
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/secure-code-validation/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/security-audits-and-compliance
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/test-center-of-excellence/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.

URL	https://virtuestech.com/services/vulnerability-assessment/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/zero-trust-network-assessments/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/sitemap.xml
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/embed/
Method	GET
Parameter	Content-Security-Policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/wp-admin/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/wp-admin/admin-ajax.php

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.

URL	https://virtuestech.com/wp-login.php
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/contact/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	content-security-policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/cyber-resilience-testing/

Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.

URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/wp-comments-post.php
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
Instances	233
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	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://virtuestech.com
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.

URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=1025
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=1039
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=1050
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=1078
Method	GET
Parameter	content-security-policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13377
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13410
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13420
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13428
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13434
Method	GET

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13610
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13621
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13645
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=13749
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=14364

Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=14382
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=15119
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=1522
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=1545
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.

URL	https://virtuestech.com/?p=188
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=18967
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=19359
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=19466
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=19537
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20009
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20339
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20343
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20365
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20587
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20606
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20670
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20732
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20738
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20754
Method	GET
Parameter	content-security-policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=20790
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=21232
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=21263
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=21974
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22176
Method	GET

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22561
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22566
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22571
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22576
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22581

Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22586
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22591
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22675
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22680
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.

URL	https://virtuestech.com/?p=22685
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22690
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22695
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22700
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=22708
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=256
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=271
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=3500
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=439
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=474
Method	GET
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?p=5664
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/?page_id=20760
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/about/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/about/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/advisorytransformation
Method	GET

Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/ai-driven-test-automation-2/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/ai-driven-test-automation/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/atlas/embed/

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/blogs/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.

URL	https://virtuestech.com/blogs/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/blogs/page/2/?ajaxify=1
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/careers/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/careers/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/category/uncategorized/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/contact
Method	GET
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/contact/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/contact/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/continuous-quality-engineering
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/cybersecurity-services/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/embed/
Method	GET
Parameter	content-security-policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/industries/
Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/industries/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/insights/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/accessibility-usability-testing/

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/accessibility-usability-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/advisory-and-transformation/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.

URL	https://virtuestech.com/services/agile-and-devops-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/ai-driven-test-automation/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-security-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-testing-services
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-testing-services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/business-experience-validation/embed/
Method	GET
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-native-application-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-security-testing
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-security-testing/embed/
Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/compliance-and-security-audits/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/continuous-quality-engineering

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/continuous-quality-engineering/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/cyber-resilience-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.

URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/data-driven-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/devsecops-integration/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/iot-security-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/managed-soc-services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/manual-testing-services/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/mobile-security-testing/embed/
Method	GET
Parameter	content-security-policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/penetration-testing/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/performance-engineering-monitoring/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/performance-testing-services
Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/secure-code-validation/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/security-audits-and-compliance
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/embed/

Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/test-center-of-excellence/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/vulnerability-assessment/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.

URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/zero-trust-network-assessments/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/sitemap.xml
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/embed/
Method	GET
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	content-security-policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/embed/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/embed/

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/embed/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/wp-admin/
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/wp-admin/admin-ajax.php
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.

URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/wp-login.php
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	content-security-policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/contact/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST

Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/cloud-security-testing/

Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.

URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests

Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	Content-Security-Policy
Attack	

Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	content-security-policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/wp-comments-post.php
Method	POST
Parameter	Content-Security-Policy

Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
Instances	233
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	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://virtuestech.com/xmlrpc.php
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/xmlrpc.php?rsd
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	2
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/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

MEDIUM	MISSING ANTI-CLICKJACKING HEADER
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://virtuestech.com
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	x-frame-options
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/about/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/about/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation-2/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/atlas/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	x-frame-options
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/best-practices-for-effective-software-testing/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/blogs/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/blogs/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/blogs/page/2/?ajaxify=1
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/careers/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/careers/embed/

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/uncategorized/
Method	GET
Parameter	x-frame-options
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/contact/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/contact/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/embed/

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/industries/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/industries/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/accessibility-usability-testing/embed/
Method	GET
Parameter	x-frame-options
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/advisory-and-transformation/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/agile-and-devops-testing/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/ai-driven-test-automation/embed/

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-security-testing/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-testing-services/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	x-frame-options
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/business-experience-validation/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-native-application-testing/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/compliance-and-security-audits/

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/compliance-and-security-audits/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering/embed/
Method	GET
Parameter	x-frame-options
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cyber-resilience-testing/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/data-driven-testing/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/devsecops-integration/embed/

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-security-testing/embed/
Method	GET
Parameter	x-frame-options
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/embed/

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/penetration-testing/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	x-frame-options
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/secure-code-validation/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/test-center-of-excellence/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/vulnerability-assessment/

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/vulnerability-assessment/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/zero-trust-network-assessments/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	x-frame-options
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/embed/
Method	GET
Parameter	x-frame-options
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-do-the-mobile-manual-test/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/embed/

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/contact/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	x-frame-options
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/business-experience-validation/

Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	x-frame-options
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/

Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	x-frame-options
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
Instances	148
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021

WASC Id	15
Plugin Id	10020

MEDIUM	VULNERABLE JS LIBRARY
Description	The identified library appears to be vulnerable.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/jquery-ui/jquery-ui.min.js
Method	GET
Parameter	
Attack	
Evidence	/*! jQuery UI - v1.13.1
Other Info	The identified library jquery-ui, version 1.13.1 is vulnerable. CVE-2022-31160 https://github.com/advisories/GHSA-h6gj-6jjq-h8g9 https://github.com/jquery/jquery-ui/commit/8cc5bae1caa1fcf96bf5862c5646c787020ba3f9 https://nvd.nist.gov/vuln/detail/CVE-2022-31160 https://github.com/jquery/jquery-ui/issues/2101
Instances	1
Solution	Upgrade to the latest version of the affected library.
Reference	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
CWE Id	1395
WASC Id	
Plugin Id	10003

LOW	COOKIE NO HTTPONLY FLAG
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://virtuestech.com/wp-login.php
Method	GET
Parameter	wordpress_test_cookie
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	

URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET
Parameter	wordpress_test_cookie
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	wordpress_test_cookie
Attack	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	wordpress_test_cookie
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	wordpress_test_cookie
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
Instances	5
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

LOW	COOKIE WITHOUT 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://virtuestech.com/wp-login.php
Method	GET
Parameter	wordpress_test_cookie
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET
Parameter	wordpress_test_cookie
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	wordpress_test_cookie
Attack	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	wordpress_test_cookie
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	POST

Parameter	wordpress_test_cookie
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://tools.ietf.org/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://virtuestech.com
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="c353a17fd30e717bbd6f0e6d-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="fd1cac23c9bf4fcdd645dd8e-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="1ddc0021b2e8f5359a544b4d-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="502ec4b3b2d2b8e450180cd9-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="254c414238f4820745692140-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="a05ad4f28bec485e325315f3-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="5bfeaad41c9edcb3c805d759-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="719d9a1de12f5ea8a132acf1-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="3f0f7710d6bbbfb692255db2-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="778499b863d0ac052a8c0970-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="bd127a0a3e9c011b10818d7a-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="2e3a56436d7e475939565b96-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="e97da55fa30cdb14b6dbb000-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="c515160862a40c9dc73795ed-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="2cff686d42508a148feccf7d-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/?page_id=20760
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="ec20886b878be9b4608e817d-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/about/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="1afa095dc9940bebaa5fa2be-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/advisorytransformation
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="770b978041fa4f6e3ddde907-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="7c119440ef73503b73bfd9ba-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="fe86516d8e39e83a26e72a33-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="0fe780e6d16af3caba52a55b-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="6eec3c9192ec99e425af371f-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/blogs/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="ec8026bf7239280a950fcc4d-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/careers/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="fd7672ef7f63d213318a3905-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="db11d807e2b72c409c60fe84-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/category/digital-assurance/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="bfe8a7e0ba42674831782030-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="0da95af87804c0c9b452c70c-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="8d735122433f95adec601221-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/category/uncategorized/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="c65fcbc8e8c522e0025262c2-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/contact/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="e051116a452830b46a5b610f-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/cybersecurity-services/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="b41deac341404483b54e31f9-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="0e2b9cc2d6193f0e95c3c9ca-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="04dfe7ac822916b511909ea9-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/industries/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="3c3224f1413300c6a40f56e5-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/insights/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="30900b00b632378bc144e115-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="3f903292370bd6e69828d268-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="a1bb93cf09916819cc8a8802-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="90ebf80f51da3d3783bb4f70-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="1270ca77369746d6dd1a388e-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="b468cfe1c116adf8c8d17fc7-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="946acba4388917f7033f288d-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/api-testing-services/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="7bf6acd35e4f88432454f8f0-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="a70202ef80ba39e6e5373599-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="4949563b665bb45c9ec1e2d2-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="9985465023456cd152ab1bba-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="f67e501244e96a6cd00ba74b-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="089fd5c82fa49465177ea16c-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="3b8e25ce5743cb7bb9ece49e-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="4a29d53f8e9ea23eb40d4427-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="abf70195200402816379c102-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="14c1fe39094ee401c347fc42-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="d02bcfb1e9c620af3d337821-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="2d82873c8f81a9fb613987eb-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="28bff7cb97613484559f69f3-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="4e3c09332eb6e607224a830c-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="e6192b3956b0c86ee3e922a4-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="132d9442aa46e0ad0914fedf-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="2fb65eb1b8627f4d68495e90-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/performance-Engineering-Monitoring/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="3df61e595f3bd71a2434e76a-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/performance-testing-services
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="07888964462fc9141125d4c6-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="820fca8b415af4549a20d125-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/security-audits-and-compliance
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="c7ddeb36b26a8c8a1f36633f-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="23b45d71fc2e809eafbf9cc5-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="f2cf173f38c90ca18c33a67d-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="d7eee4ff7271fae180cfdbc1-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="becd178862b01383bac389ca-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="644479ef650009f5191ebf89-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="87fd7a8cff0f74311d7c0515-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="3de2c8bae3b03793637b2a35-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/tag/software-testing/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="ade6ae44e3a4d349c1d1e1c3-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="7df69b3a2f4e45b7dc4d62a5-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="12a24bd792dfcc0f2fb1e0dc-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="fbc0772384d54e07816f8fbb-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="01ff62fa7c2680d4a57ef6f5-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="7e1ede2aee9fe8fbc534bb37-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="805bbdc6bf598b280ca4f63c-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="5f9c4c998f2169929652058a-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="84a3d2811844f1c6977f5cd6-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="269ae79cbf21262041180193-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="039f64db190f8b736df34d3a-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="020686b2395b9131ab47c3fa-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png
Method	GET

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="2a4c2ba43b2d9c601c4d7ff0-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="a1a0c6237593e2f75d76b874-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="36b42e16adeae2a7b8a4f448-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="fac3e278f74a5d6a6e2ab569-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/contact/
Method	POST

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="f93bc48726a5eef11f032b40-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="e363c343dce4d4c8cd776b38-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="619183f399dc486a2a50211f-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="bea34d0daa18cdb6162b0f90-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="0c6416c2304fc7353ae46d51-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="bad1294ce8368b53df6cf7ba-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="e82c61fd4ccc5f3a72e474c2-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="b6daba9016a3581bb6b9ecdf-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="78bd362b9bcc1deed316cc4e-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="263e533ff1f486bb9889d256-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="8a7799b3f3dae86d4c65b88d-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="4dd243578ec15c157635bcf7-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="b5363cb0972138ee3601a239-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="c293f3bdf23cd9edfb54f337-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="556ba1a6d7f8b0b22074b463-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="d1c206efbe99d088dfa216ac-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="1acd2bae5544e72d5c8070d8-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="05152e83d0deff9d920d19f7-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="3cdf95c7eb375f53b991b014-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="251a96d0972ebdf9c5cb8e93-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="ffa5711c8f90ca0e8e1fe819-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="ca8cb48aa089945710982774-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="a1f13c0082f987c82a795860-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/performance-Engineering-Monitoring/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="d451241baccd4f46ae3d216a-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="91af08a462c7cc1caf9be348-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="e2ae04857a573c79fdd79dcd-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="99fb9978b0425b9cfe0d3f4f-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="647faf0e171c54cc1e761d57-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST

Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0
Attack	
Evidence	<script type="9ca3087ed7261142032d12b6-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi&ver=3.0" id="google-recaptcha-js"> </script>
Other Info	
Instances	115
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

LOW	**SERVER LEAKS INFORMATION VIA "X-POWERED-BY" HTTP RESPONSE HEADER FIELD(S)**
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	https://virtuestech.com
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	

Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	

Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=1025
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=1039
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=1050
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=1078
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/?p=13377
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=13410
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=13420
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=13428
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=13434
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=13610
Method	GET
Parameter	

Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=13621
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=13645
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=13749
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=14364
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=14382
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/?p=15119
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=1522
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=1545
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=188
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=18967
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=19359
Method	GET
Parameter	

Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=19466
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=19537
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=20009
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=20339
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=20343
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/?p=20365
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=20587
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=20606
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=20670
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=20732
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=20738
Method	GET
Parameter	

Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=20754
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=20790
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=21232
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=21263
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=21974
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/?p=22176
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=22561
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=22566
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=22571
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=22576
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=22581
Method	GET

Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=22586
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=22591
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=22675
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=22680
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=22685
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/?p=22690
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=22695
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=22700
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=22708
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=256
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=271
Method	GET

Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=3500
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=439
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=474
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?p=5664
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/?page_id=20760
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/about/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/about/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/advisorytransformation
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation-2/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation/
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/atlas/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/author/virtuestech/feed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/best-practices-for-effective-software-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/best-practices-for-effective-software-testing/feed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/blogs/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/blogs/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/blogs/page/2/?ajaxify=1
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/careers/
Method	GET

Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/careers/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/category-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/category/cyber-security/feed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/category/digital-assurance/feed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/category/quality-engineering/feed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/category/software-testing/feed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/category/uncategorized/
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/category/uncategorized/feed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/comments/feed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/contact
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/contact/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/contact/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/continuous-quality-engineering
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/cybersecurity-services/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/feed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/embed/
Method	GET

Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/feed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/industries/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/industries/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/insights/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/liquid-footer-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/liquid-header-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/liquid-mega-menu-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/page-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/post-sitemap.xml
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/accessibility-usability-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/advisory-and-transformation/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/agile-and-devops-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/ai-driven-test-automation/embed/
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/api-security-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/api-testing-services
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/api-testing-services/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/business-experience-validation/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/cloud-native-application-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET

Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/compliance-and-security-audits/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/cyber-resilience-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET

Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/data-driven-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/devsecops-integration/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/iot-security-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET

Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/penetration-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/performance-Engineering-Monitoring/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/performance-testing-services
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/secure-code-validation/embed/
Method	GET

Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/security-audits-and-compliance
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/test-center-of-excellence/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/vulnerability-assessment/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/zero-trust-network-assessments/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/sitemap_index.xml
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/tag/automation-testing/feed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/tag/integration-testing/feed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/tag/manual-testing/feed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/tag/software-testing/feed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/tag/test-automation/feed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET

Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/feed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/embed/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET

Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/why-do-the-mobile-manual-test/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/embed/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-admin/
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-admin/admin-ajax.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dfooter
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dvst-main-footer
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dheader
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dnew-header
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dvst-main-header
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dcs-menu
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Delementor-1025
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dis-menu
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dmenu-cybersecurity
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dqe-menu
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservice-offerings
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservices
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dtaas-menu
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fabout%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fai-driven-test-automation-2%2F
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fatlas%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fbest-practices-for-effective-software-testing%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fblogs%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcareers%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcontact%2F
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-performance-testing-and-monitoring%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Findustries%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Faccessibility-usability-testing%2F

Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fadvisory-and-transformation%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fagile-and-devops-testing%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fai-driven-test-automation%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-testing-services%2F

Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fbusiness-experience-validation%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-native-application-testing%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcompliance-and-security-audits%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcomprehensive-test-automation-framework%2F

Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcontinuous-quality-engineering%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcyber-resilience-testing%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdata-driven-testing%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdevsecops-integration%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-and-embedded-systems-testing%2F

Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanaged-soc-services%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanual-testing-services%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmobile-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fpenetration-testing%2F

Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fperformance-engineering-monitoring%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fsecure-code-validation%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fshift-left-and-shift-right-testing%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Ftest-center-of-excellence%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fvulnerability-assessment%2F

Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fzero-trust-network-assessments%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Futilizing-mobile-technology-in-the-field%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fvulnerability-assessments-penetration-testing-cybersecurity%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-exploratory-testing-why-and-when-do-we-need-it%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-integration-testing-and-types-approach%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhy-cloud-security-testing-is-essential%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhy-do-the-mobile-manual-test%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhy-is-independent-software-testing-vital-to-successful-applications-in-any-industry%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dfooter
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dvst-main-footer
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dheader
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dnew-header
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dvst-main-header
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dcs-menu
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Delementor-1025
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dis-menu
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dmenu-cybersecurity
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dqe-menu
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservice-offerings
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservices
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dtaas-menu
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fabout%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fai-driven-test-automation-2%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fatlas%2F

Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fbest-practices-for-effective-software-testing%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fblogs%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fcareers%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fcontact%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry%2F
Method	GET
Parameter	

Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-performance-testing-and-monitoring%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Findustries%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Faccessibility-usability-testing%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fadvisory-and-transformation%2F
Method	GET
Parameter	
Attack	

Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fagile-and-devops-testing%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fai-driven-test-automation%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-testing-services%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fbusiness-experience-validation%2F
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-native-application-testing%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcompliance-and-security-audits%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcomprehensive-test-automation-framework%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcontinuous-quality-engineering%2F
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcyber-resilience-testing%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdata-driven-testing%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdevsecops-integration%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-and-embedded-systems-testing%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-security-testing%2F
Method	GET
Parameter	
Attack	

Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanaged-soc-services%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanual-testing-services%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmobile-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fpenetration-testing%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fperformance-engineering-monitoring%2F
Method	GET
Parameter	
Attack	

Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fsecure-code-validation%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fshift-left-and-shift-right-testing%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Ftest-center-of-excellence%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fvulnerability-assessment%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fzero-trust-network-assessments%2F
Method	GET
Parameter	
Attack	

Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Futilizing-mobile-technology-in-the-field%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fvulnerability-assessments-penetration-testing-cybersecurity%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-exploratory-testing-why-and-when-do-we-need-it%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-integration-testing-and-types-approach%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhy-cloud-security-testing-is-essential%2F
Method	GET
Parameter	
Attack	

Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhy-do-the-mobile-manual-test%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhy-is-independent-software-testing-vital-to-successful-applications-in-any-industry%2F
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/categories/1
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/categories/30
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/categories/34
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/wp-json/wp/v2/categories/35
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/categories/36
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/13610
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/13621
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/13645
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/13749
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/14364
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/14382
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/188
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/19359
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/19466
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/19537
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20009
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20587
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20606
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20670
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20732
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20738
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20754
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20790
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/21974
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22561
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22566
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22571
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22576
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22581
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22586
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22591
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22675
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22680
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22685
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22690
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22695
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27

Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22700
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22708
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22906
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/256
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/271
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13377

Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13410
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13420
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13428
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13434
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/15119
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/21232
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/21263
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/22176
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/3500
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/28
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/wp-json/wp/v2/tags/29
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/31
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/32
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/33
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/users/1
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-login.php
Method	GET
Parameter	

Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/contact/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	

Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	

Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	

URL	https://virtuestech.com/services/performance-Engineering-Monitoring/
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST

Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-comments-post.php
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.27
Other Info	
Instances	435
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

CWE Id	497
WASC Id	13
Plugin Id	10037

LOW	**STRICT-TRANSPORT-SECURITY HEADER NOT SET**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://virtuestech.com
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-header=header

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?page_id=20760
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/about/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/about/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/advisorytransformation
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation-2/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/atlas/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/author/virtuestech/feed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/best-practices-for-effective-software-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/best-practices-for-effective-software-testing/feed/
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/blogs/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/blogs/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/blogs/page/2/?ajaxify=1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/careers/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/careers/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category-sitemap.xml
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/cyber-security/feed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/digital-assurance/feed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/quality-engineering/feed/
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/software-testing/feed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/uncategorized/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/uncategorized/feed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/cdn-cgi/scripts/7d0fa10a/cloudflare-static/rocket-loader.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/cdn-cgi/styles/cf.errors.css

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/cdn-cgi/styles/cf.errors.ie.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/comments/feed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/contact/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/contact/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/cybersecurity-services/
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/feed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/feed/
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/industries/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/industries/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/insights/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/liquid-footer-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/liquid-header-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/liquid-mega-menu-sitemap.xml
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/page-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/post-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/accessibility-usability-testing/embed/
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/advisory-and-transformation/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/agile-and-devops-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/ai-driven-test-automation/embed/
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-security-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-testing-services/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/services/business-experience-validation/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-native-application-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/services/compliance-and-security-audits/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/services/cyber-resilience-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/data-driven-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/devsecops-integration/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/embed/
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-security-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/embed/
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/penetration-testing/embed/

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/performance-testing-services
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/secure-code-validation/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/security-audits-and-compliance

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/test-center-of-excellence/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/services/vulnerability-assessment/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/zero-trust-network-assessments/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/sitemap_index.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/automation-testing/feed/
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/integration-testing/feed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/manual-testing/feed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/software-testing/feed/
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/test-automation/feed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/embed/
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/feed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-do-the-mobile-manual-test/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-admin/admin-ajax.php
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-admin/css/forms.min.css?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-admin/css/l10n.min.css?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-admin/css/login.min.css?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-admin/js/password-strength-meter.min.js?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-admin/js/user-profile.min.js?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=6.0.5
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/includes/js/index.js?ver=6.0.5
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/includes/swv/js/index.js?ver=6.0.5
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/modules/recaptcha/index.js?ver=6.0.5
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/css/widget-divider.min.css?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/css/widget-image.min.css?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/css/widget-social-icons.min.css?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/css/widget-spacer.min.css?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/js/frontend-modules.min.js?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/all.min.css?ver=3.28.3
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/v4-shims.min.css?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/lib/font-awesome/js/v4-shims.min.js?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/hub-core/extras/redux-framework/redux-core/assets/css/extendify-utilities.css?ver=4.4.12.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/hub-elementor-addons/assets/css/blog/blog-single/blog-single-base.css?ver=5.0.7
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/hub-elementor-addons/assets/css/pages/not-found.css?ver=5.0.7
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/plugins/hub-elementor-addons/assets/css/theme-elementor.min.css?ver=5.0.7
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/assets/dummy.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/css/rs6.css?ver=6.7.19
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/fonts/revicons/revicons.woff?5510888
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/js/rbtools.min.js?ver=6.7.19
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/js/rs6.min.js?ver=6.7.19
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/css/elements/base/typography.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/js/theme.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/bootstrap/css/bootstrap.min.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/bootstrap/js/bootstrap.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/fastdom/fastdom.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/flickity/flickity-fade.min.js
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/flickity/flickity.pkgd.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/fontfaceobserver.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/fresco/css/fresco.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/fresco/js/fresco.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/gsap/minified/gsap.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/gsap/minified/ScrollTrigger.min.js
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/gsap/utils/SplitText.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/intersection-observer.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/isotope/isotope.pkgd.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/isotope/packery-mode.pkgd.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/jquery-ui/jquery-ui.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/lazyload.min.js
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/liquid-icon/lqd-essentials/fonts/lqd-essentials.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/liquid-icon/lqd-essentials/lqd-essentials.min.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/liquid-icon/lqd-essentials/lqd-essentials.min.css?ver=1.0.0
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/lity/lity.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/particles.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/tinycolor-min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/themes/hub/style.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-icon-1.svg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1-1024x276.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1-1536x414.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1-2048x552.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1-300x81.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech_LOGO-1.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/Integration-testing-1-300x150.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/Integration-testing-1-640x350.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/Integration-testing-1.jpg
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/software-testing-trends-1-300x150.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/software-testing-trends-1-640x364.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/software-testing-trends-1-720x400.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/software-testing-trends-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues-e1678973425717-1-300x173.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues-e1678973425717-1.jpg
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1665455409401-1024x791.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1665455409401-300x232.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1665455409401.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer.png
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1-150x150.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1-300x300.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1-320x320.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1-760x760.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/bugzilla-e1680261726322-1.png
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1-300x150.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1-480x300.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1-640x364.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1-720x450.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Energy-Utilities-1.jpg

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Financial-Services-1-300x225.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Financial-Services-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Healthcare-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/HP-Quality-Center-e1680262577123-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Independent-Quality-Assurance-Testing-1-300x150.png
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Independent-Quality-Assurance-Testing-1.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Jira-e1680262548454-1.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/MantisBT-Logo-1-e1680262729435-1.webp
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Mobile-app-test-1-150x150.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Mobile-app-test-1-300x300.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Mobile-app-test-1-320x320.jpeg
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Mobile-app-test-1.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/MobileAppTesting-1-300x150.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/MobileAppTesting-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/testlink-e1680261675504-1.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/TestRail-e1680261609742-1.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/Travel-1.jpg
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/What-is-Exploratory-Testing_-1-1-1024x419.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/What-is-Exploratory-Testing_-1-1-300x123.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/What-is-Exploratory-Testing_-1-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/03/why-work-here-2.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/04/Cyber_Security-1-e1730117952973-300x195.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/04/Cyber_Security-1-e1730117952973-640x364.jpg
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/04/Cyber_Security-1-e1730117952973.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/04/Digital-Assurance-e1682654035504-1-150x150.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/04/Digital-Assurance-e1682654035504-1-300x300.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/04/Digital-Assurance-e1682654035504-1-320x320.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/04/Digital-Assurance-e1682654035504-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/05/Engineering-Home-1-1-300x200.jpg
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/05/Engineering-Home-1-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/05/Services_banner_QE-e1684337302375-1-1024x353.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/05/Services_banner_QE-e1684337302375-1-300x103.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/05/Services_banner_QE-e1684337302375-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/06/Customer-Satisfaction-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/uploads/2023/06/Security-Testing-Services-1-e1731289538553.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate002-e1690716237786-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate004-1-e1727692153719-300x158.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate004-1-e1727692153719.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate005-e1690732096817-1-300x153.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate005-e1690732096817-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/uploads/2023/07/VST-Home-0005-2-1-150x150.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/07/VST-Home-0005-2-1-300x300.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/07/VST-Home-0005-2-1-320x320.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2023/07/VST-Home-0005-2-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/A-20-1-e1730195345387-223x300.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/A-20-1-e1730195345387.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/badge2.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-1024x433.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-1536x650.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-2048x867.jpg

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-300x127.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-768x325.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/E-commerce-and-Retail-e1730958682357.webp
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/EDTech-e1730958663954.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/uploads/2024/10/img-2@2x-1-248x300.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/img-2@2x-1-847x1024.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/img-2@2x-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/IoT-and-Smart-Devices-e1730958550602.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Media-and-Entertainment-e1730958634556.webp
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-18-at-3.22.07-PM-e1729764887836.jpeg
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-18-at-3.22.10-PM-e1729764869724.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-23-at-12.21.03-PM.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-24-at-13.11.54-5-e1729764673300.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-24-at-3.27.27-PM-1-e1729764734764.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-24-at-3.27.28-PM-3.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.23.26.jpeg
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.24.25.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.30.16.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.31.29.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.32.05.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.47.28.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-29-at-16.22.27.jpeg
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-1024x495.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-1536x742.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-2048x989.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-300x145.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-480x300.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-640x364.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-720x510.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/AccelESG-logo.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Advisory-Transformationv03-e1731289439749.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/ATLAS-Banner-480x300.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/uploads/2024/11/ATLAS-Banner-640x350.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/ATLAS-Banner-720x350.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/berribot-logo.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/CTE.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/HackerEarth-Logo.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-1024x549.jpeg
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-300x161.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-480x300.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-640x364.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-720x510.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/kagoollogo.svg

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Leanpitch-1.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/octalFrames_logo.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02-1024x418.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02-1536x627.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02-2048x837.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02-300x123.jpeg

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/preferredhcny-logo.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/PXL_20241030_110509234.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/PXL_20241030_124938251.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/rollick-logo.png
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/seller-legend-300x45-1.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Test-Automationv002-300x210.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Test-Automationv002.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/the-credit-pros--300x34.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/the-credit-pros-.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Unocoin-logo-1.png
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/VSoft-Logo-300x102.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/VSoft-Logo.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-Culture-and-Values-300x185.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-Culture-and-Values.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home001.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home002.png
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home003.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home1.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home2.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home3.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/westoninfosec-1.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/12/Carees_VSt_003.jpeg
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/12/software-testing_advisory_007.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/12/software-testing_cs_006.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/12/software-testing_QE_005.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/12/VST_Home_001.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/12/VST_Home_002.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/12/WhatsApp-Image-2024-11-28-at-16.12.24.jpeg
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2025/01/IMG_20250106_164122-e1737460521938.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2025/01/IMG_20250106_184150-e1737460619584.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2025/04/CS_Service_01.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01-1024x465.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01-1536x698.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01-2048x931.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01-300x136.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01.jpeg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/css/custom-apple-webkit.min.css?ver=1744173930
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/css/custom-frontend.min.css?ver=1744173930
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/inter.css?ver=1743442410
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/opensans.css?ver=1743442392
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/poppins.css?ver=1743442395
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/roboto.css?ver=1743442383
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/robotocondensed.css?ver=1744093863
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l0uumjng.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l1uumjng.woff2
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l2uumjng.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l3uumjng.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l5uum.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l6uumjng.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l9uumjng.woff2
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia0zl7suc.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia1pl7suc.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia1zl7.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia25l7suc.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia2jl7suc.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia2pl7suc.woff2

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia2zl7suc.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqw106f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwt06f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwte6f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwtk6f15m.woff2
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwtu6f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwu06f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwuk6f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwuu6f.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwvu6f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwxu6f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovts-muw.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovts2mu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtscmu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtsgmu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtskmu1ab.woff2

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtsomu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtsumu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtsymu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtugmu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtvomu1ab.woff2
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxiayp8kv8jhgfvrjjlme0tcmpi.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxiayp8kv8jhgfvrjjlme0tmmpkzsq.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlbt5z1jlfc-k.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlbt5z1xlfq.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlcz7z1jlfc-k.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlcz7z1xlfq.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrldd4z1jlfc-k.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrldd4z1xlfq.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrldz8z1jlfc-k.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrldz8z1xlfq.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlej6z1jlfc-k.woff2

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlej6z1xlfq.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlfj_z1jlfc-k.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlfj_z1xlfq.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlgt9z1jlfc-k.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlgt9z1xlfq.woff2
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm111vf9eo.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm111vgdeoceg.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm21lvf9eo.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm21lvgdeoceg.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm81xvf9eo.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm81xvgdeoceg.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmg1hvf9eo.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmg1hvgdeoceg.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmr19vf9eo.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmr19vgdeoceg.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmv1pvf9eo.woff2

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmv1pvgdeoceg.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmy15vf9eo.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmy15vgdeoceg.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxieyp8kv8jhgfvrjjfecg.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxieyp8kv8jhgfvrjjnecmne.woff2
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrjjluchta.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrjjlufntakpy.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrlptuchta.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrlptufntakpy.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkahkawzu.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkankawzu.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkbnka.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkbxkawzu.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkc3kawzu.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkchkawzu.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkcnkawzu.woff2

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkcxkawzu.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkenkawzu.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3-ubgee.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3cubgee.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3gubgee.woff2
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3iubgee.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3kubgee.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3oubgee.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3yuba.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluamawcubgee.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluamaxkubgee.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19elaam9uvi.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19elagm9uvi.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19elaqm9uvi.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19elawm9uvi.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19elcwm9uvi.woff2

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19eldam9uvi.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19eldwm9.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-19-7drs5.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-1927drs5.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-1967drs5.woff2
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-19a7drs5.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-19g7drs5.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-19k7dq.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-19y7drs5.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/css/buttons.min.css?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-includes/css/dashicons.min.css?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/css/dist/block-library/style.min.css?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/js/clipboard.min.js?ver=2.0.11
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/js/comment-reply.min.js?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/js/dist/a11y.min.js?ver=3156534cc54473497e14
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/js/dist/dom-ready.min.js?ver=f77871ff7694fffea381
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-includes/js/dist/hooks.min.js?ver=4d63a3d491d11ffd8ac6
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/js/dist/i18n.min.js?ver=5e580eb46a90c2b997e6
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/js/imagesloaded.min.js?ver=5.0.0
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/js/jquery/ui/core.min.js?ver=1.13.3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/js/underscore.min.js?ver=1.13.7
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/js/wp-util.min.js?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-includes/js/zxcvbn-async.min.js?ver=1.0
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dfooter
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dvst-main-footer
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dheader
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dnew-header
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dvst-main-header
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dcs-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Delementor-1025
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dis-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dmenu-cybersecurity
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dqe-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservice-offerings

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservices
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dtaas-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fabout%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fai-driven-test-automation-2%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fatlas%2F
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fbest-practices-for-effective-software-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fblogs%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcareers%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcontact%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry%2F
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-performance-testing-and-monitoring%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Findustries%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Faccessibility-usability-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fadvisory-and-transformation%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fagile-and-devops-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fai-driven-test-automation%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-testing-services%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fbusiness-experience-validation%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-native-application-testing%2F

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcompliance-and-security-audits%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcomprehensive-test-automation-framework%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcontinuous-quality-engineering%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcyber-resilience-testing%2F
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdata-driven-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdevsecops-integration%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-and-embedded-systems-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanaged-soc-services%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanual-testing-services%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmobile-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fpenetration-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fperformance-engineering-monitoring%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fsecure-code-validation%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fshift-left-and-shift-right-testing%2F

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Ftest-center-of-excellence%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fvulnerability-assessment%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fzero-trust-network-assessments%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Futilizing-mobile-technology-in-the-field%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fvulnerability-assessments-penetration-testing-cybersecurity%2F
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-exploratory-testing-why-and-when-do-we-need-it%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-integration-testing-and-types-approach%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhy-cloud-security-testing-is-essential%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhy-do-the-mobile-manual-test%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhy-is-independent-software-testing-vital-to-successful-applications-in-any-industry%2F
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dfooter
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dvst-main-footer
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dheader
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dnew-header
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dvst-main-header
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dcs-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Delementor-1025
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dis-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dmenu-cybersecurity
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dqe-menu

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservice-offerings
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservices
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dtaas-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fabout%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fai-driven-test-automation-2%2F
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fatlas%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fbest-practices-for-effective-software-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fblogs%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fcareers%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fcontact%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry%2F
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-performance-testing-and-monitoring%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Findustries%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Faccessibility-usability-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fadvisory-and-transformation%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fagile-and-devops-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fai-driven-test-automation%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-testing-services%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fbusiness-experience-validation%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-native-application-testing%2F

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcompliance-and-security-audits%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcomprehensive-test-automation-framework%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcontinuous-quality-engineering%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcyber-resilience-testing%2F
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdata-driven-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdevsecops-integration%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-and-embedded-systems-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanaged-soc-services%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanual-testing-services%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmobile-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fpenetration-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fperformance-engineering-monitoring%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fsecure-code-validation%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fshift-left-and-shift-right-testing%2F

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Ftest-center-of-excellence%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fvulnerability-assessment%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fzero-trust-network-assessments%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Futilizing-mobile-technology-in-the-field%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fvulnerability-assessments-penetration-testing-cybersecurity%2F
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-exploratory-testing-why-and-when-do-we-need-it%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-integration-testing-and-types-approach%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhy-cloud-security-testing-is-essential%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhy-do-the-mobile-manual-test%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhy-is-independent-software-testing-vital-to-successful-applications-in-any-industry%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-json/wp/v2/categories/1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/categories/30
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/categories/34
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/categories/35
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/categories/36
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/13610
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/13621
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/13645
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/13749
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/14364
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/14382
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/188
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/19359
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/19466
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/19537
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20009
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20587
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20606
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20670
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20732
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20738
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20754
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20790
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/21974
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22561
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22566
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22571
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22576
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22581
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22586

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22591
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22675
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22680
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22685
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22690
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22695

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22700
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22708
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22906
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/256
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/271
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13377
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13410
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13420
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13428
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13434
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/15119
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/21232
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/21263
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/22176
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/3500
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/28
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/29
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/31
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/32
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/33
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/users/1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-login.php
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/xmlrpc.php
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/xmlrpc.php?rsd
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/atlas/

Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/contact/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-security-testing/

Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-comments-post.php
Method	POST

Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
Instances	720
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

LOW	**TIMESTAMP DISCLOSURE - UNIX**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://virtuestech.com
Method	GET
Parameter	
Attack	
Evidence	1743442383

Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com
Method	GET
Parameter	
Attack	
Evidence	1744093863
Other Info	1744093863, which evaluates to: 2025-04-08 12:01:03.
URL	https://virtuestech.com
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.

URL	https://virtuestech.com/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/
Method	GET
Parameter	
Attack	
Evidence	1744093863
Other Info	1744093863, which evaluates to: 2025-04-08 12:01:03.
URL	https://virtuestech.com/

Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET

Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	

Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	
Attack	

Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	
Attack	
Evidence	1744173930

Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.

URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025

Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET

Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	

Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	
Attack	

Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	
Attack	
Evidence	1743442383

Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.

URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu

Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/?page_id=20760
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/?page_id=20760
Method	GET

Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/?page_id=20760
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/?page_id=20760
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/?page_id=20760
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/about/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/about/
Method	GET
Parameter	

Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/about/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/about/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/about/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/advisorytransformation
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/advisorytransformation
Method	GET
Parameter	
Attack	

Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/advisorytransformation
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/advisorytransformation
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/advisorytransformation
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	
Attack	
Evidence	1743442392

Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/ai-driven-test-automation-2/embed/
Method	GET
Parameter	
Attack	
Evidence	1606377621
Other Info	1606377621, which evaluates to: 2020-11-26 13:30:21.
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	
Attack	
Evidence	1743442383

Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/atlas/embed/
Method	GET
Parameter	
Attack	
Evidence	1951014219
Other Info	1951014219, which evaluates to: 2031-10-29 09:53:39.

URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/

Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/embed/

Method	GET
Parameter	
Attack	
Evidence	1821402764
Other Info	1821402764, which evaluates to: 2027-09-20 06:42:44.
URL	https://virtuestech.com/blogs/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/blogs/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/blogs/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/blogs/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/blogs/
Method	GET

Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/careers/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/careers/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/careers/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/careers/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/careers/
Method	GET
Parameter	

Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	
Attack	

Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	
Attack	
Evidence	1744173930

Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.

URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/category/uncategorized/

Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/category/uncategorized/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/category/uncategorized/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/category/uncategorized/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/category/uncategorized/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/contact/
Method	GET

Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/contact/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/contact/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/contact/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/contact/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/cybersecurity-services/
Method	GET
Parameter	

Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/cybersecurity-services/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/cybersecurity-services/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/cybersecurity-services/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/cybersecurity-services/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	
Attack	

Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	
Attack	
Evidence	1743442383

Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/industries/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.

URL	https://virtuestech.com/industries/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/industries/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/industries/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/industries/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/insights/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/insights/

Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/insights/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/insights/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/insights/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/
Method	GET

Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	

Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	
Attack	

Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392

Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.

URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/api-security-testing/

Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/api-testing-services/
Method	GET

Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	

Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	
Attack	

Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395

Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.

URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/

Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET

Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	

Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	
Attack	

Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	
Attack	
Evidence	1743442410

Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.

URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/iot-security-testing/

Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET

Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/managed-soc-services/embed/
Method	GET
Parameter	
Attack	
Evidence	1936267305
Other Info	1936267305, which evaluates to: 2031-05-11 17:31:45.
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	

Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	
Attack	

Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410

Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	
Attack	
Evidence	1743442410

Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/performance-testing-services
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/performance-testing-services
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/performance-testing-services
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/performance-testing-services
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.

URL	https://virtuestech.com/services/performance-testing-services
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/secure-code-validation/

Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/security-audits-and-compliance
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/security-audits-and-compliance
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/security-audits-and-compliance
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/security-audits-and-compliance
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/security-audits-and-compliance
Method	GET

Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	

Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	
Attack	

Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	
Attack	
Evidence	1744173930

Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.

URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/tag/integration-testing/

Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/tag/manual-testing/
Method	GET

Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	

Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	
Attack	

Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	
Attack	
Evidence	1743442383

Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	
Attack	
Evidence	1743442383

Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.

URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/

Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/embed/
Method	GET
Parameter	
Attack	
Evidence	1778128977
Other Info	1778128977, which evaluates to: 2026-05-07 10:12:57.
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET

Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	

Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	
Attack	

Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg
Method	GET
Parameter	
Attack	
Evidence	1743442383

Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.

URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png
Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg

Method	GET
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png
Method	GET
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png
Method	GET

Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png
Method	GET
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png
Method	GET
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png
Method	GET
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/
Method	POST
Parameter	

Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/
Method	POST
Parameter	
Attack	
Evidence	1744093863
Other Info	1744093863, which evaluates to: 2025-04-08 12:01:03.
URL	https://virtuestech.com/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	
Attack	

Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	
Attack	
Evidence	1743442383

Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/contact/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.

URL	https://virtuestech.com/contact/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/contact/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/contact/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/contact/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/accessibility-usability-testing/

Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST

Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	

Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	
Attack	

Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442392

Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	
Attack	
Evidence	1743442392

Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	
Attack	
Evidence	1743442392

Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.

URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.

URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/compliance-and-security-audits/

Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST

Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	

Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	
Attack	

Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442395

Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.

URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/

Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST

Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	

Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	
Attack	

Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442410

Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.

URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/performance-engineering-monitoring/

Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/secure-code-validation/

Method	POST
Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST

Parameter	
Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	

Attack	
Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	
Attack	

Evidence	1744173930
Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	
Attack	
Evidence	1743442383
Other Info	1743442383, which evaluates to: 2025-03-31 23:03:03.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	
Attack	
Evidence	1743442392
Other Info	1743442392, which evaluates to: 2025-03-31 23:03:12.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	
Attack	
Evidence	1743442395
Other Info	1743442395, which evaluates to: 2025-03-31 23:03:15.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	
Attack	
Evidence	1743442410
Other Info	1743442410, which evaluates to: 2025-03-31 23:03:30.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	
Attack	
Evidence	1744173930

Other Info	1744173930, which evaluates to: 2025-04-09 10:15:30.
Instances	568
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

LOW	**X-CONTENT-TYPE-OPTIONS HEADER MISSING**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://virtuestech.com
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/about/
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/about/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/ai-driven-test-automation-2/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/atlas/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/author/virtuestech/feed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/best-practices-for-effective-software-testing/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/best-practices-for-effective-software-testing/feed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/blogs/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/blogs/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/blogs/page/2/?ajaxify=1
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/careers/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/careers/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/category-sitemap.xml
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/category/cyber-security/feed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/category/digital-assurance/feed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/category/quality-engineering/feed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/category/software-testing/feed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/category/uncategorized/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/category/uncategorized/feed/
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/cdn-cgi/styles/cf.errors.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/cdn-cgi/styles/cf.errors.ie.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/comments/feed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/contact/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/contact/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/feed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/feed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/industries/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/industries/embed/
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/liquid-footer-sitemap.xml
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/liquid-header-sitemap.xml
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/liquid-mega-menu-sitemap.xml
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/page-sitemap.xml
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/post-sitemap.xml
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/robots.txt
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/services/accessibility-usability-testing/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/advisory-and-transformation/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/agile-and-devops-testing/embed/
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/ai-driven-test-automation/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/api-security-testing/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/api-testing-services/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/business-experience-validation/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/cloud-native-application-testing/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/cloud-security-testing/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/compliance-and-security-audits/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/continuous-quality-engineering/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/cyber-resilience-testing/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/services/data-driven-testing/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/devsecops-integration/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/iot-security-testing/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/managed-soc-services/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/manual-testing-services/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/services/mobile-security-testing/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/penetration-testing/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/performance-engineering-monitoring/embed/
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/secure-code-validation/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/test-center-of-excellence/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/vulnerability-assessment/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/zero-trust-network-assessments/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/sitemap_index.xml
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/tag/automation-testing/feed/
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/tag/integration-testing/feed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/tag/manual-testing/feed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/tag/software-testing/feed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/tag/test-automation/feed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/feed/
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/embed/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-admin/css/forms.min.css?ver=6.7.2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-admin/css/l10n.min.css?ver=6.7.2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-admin/css/login.min.css?ver=6.7.2
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-admin/js/password-strength-meter.min.js?ver=6.7.2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-admin/js/user-profile.min.js?ver=6.7.2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=6.0.5
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/includes/js/index.js?ver=6.0.5
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/includes/swv/js/index.js?ver=6.0.5
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/modules/recaptcha/index.js?ver=6.0.5
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/css/widget-divider.min.css?ver=3.28.3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/css/widget-image.min.css?ver=3.28.3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/plugins/elementor/assets/css/widget-social-icons.min.css?ver=3.28.3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/css/widget-spacer.min.css?ver=3.28.3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/js/frontend-modules.min.js?ver=3.28.3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.28.3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.28.3
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/all.min.css?ver=3.28.3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/v4-shims.min.css?ver=3.28.3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/lib/font-awesome/js/v4-shims.min.js?ver=3.28.3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/hub-core/extras/redux-framework/redux-core/assets/css/extendify-utilities.css?ver=4.4.12.2
Method	GET
Parameter	x-content-type-options
Attack	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/hub-elementor-addons/assets/css/blog/blog-single/blog-single-base.css?ver=5.0.7
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/hub-elementor-addons/assets/css/pages/not-found.css?ver=5.0.7
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/hub-elementor-addons/assets/css/theme-elementor.min.css?ver=5.0.7
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/assets/dummy.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/css/rs6.css?ver=6.7.19
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/fonts/revicons/revicons.woff?5510888
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/js/rbtools.min.js?ver=6.7.19
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/js/rs6.min.js?ver=6.7.19
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/themes/hub/assets/css/elements/base/typography.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/js/theme.min.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/bootstrap/css/bootstrap.min.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/bootstrap/js/bootstrap.min.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/fastdom/fastdom.min.js
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/flickity/flickity-fade.min.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/flickity/flickity.pkgd.min.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/fontfaceobserver.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/fresco/css/fresco.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/fresco/js/fresco.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/gsap/minified/gsap.min.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/gsap/minified/ScrollTrigger.min.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/gsap/utils/SplitText.min.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/intersection-observer.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/isotope/isotope.pkgd.min.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/isotope/packery-mode.pkgd.min.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/jquery-ui/jquery-ui.min.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/lazyload.min.js
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/liquid-icon/lqd-essentials/fonts/lqd-essentials.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/liquid-icon/lqd-essentials/lqd-essentials.min.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/liquid-icon/lqd-essentials/lqd-essentials.min.css?ver=1.0.0
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/lity/lity.min.js
Method	GET
Parameter	x-content-type-options

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/particles.min.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/tinycolor-min.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/themes/hub/style.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-icon-1.svg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1-1024x276.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1-1536x414.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1-2048x552.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1-300x81.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech_LOGO-1.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Integration-testing-1-300x150.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Integration-testing-1-640x350.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Integration-testing-1.jpg
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/10/software-testing-trends-1-300x150.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/10/software-testing-trends-1-640x364.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/10/software-testing-trends-1-720x400.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/10/software-testing-trends-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues-e1678973425717-1-300x173.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues-e1678973425717-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1665455409401-1024x791.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1665455409401-300x232.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1665455409401.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1-150x150.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1-300x300.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1-320x320.jpg
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1-760x760.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/bugzilla-e1680261726322-1.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1-300x150.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1-480x300.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1-640x364.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1-720x450.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/2023/03/Energy-Utilities-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Financial-Services-1-300x225.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Financial-Services-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Healthcare-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/HP-Quality-Center-e1680262577123-1.jpg
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Independent-Quality-Assurance-Testing-1-300x150.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Independent-Quality-Assurance-Testing-1.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Jira-e1680262548454-1.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/MantisBT-Logo-1-e1680262729435-1.webp
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Mobile-app-test-1-150x150.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Mobile-app-test-1-300x300.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Mobile-app-test-1-320x320.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Mobile-app-test-1.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/2023/03/MobileAppTesting-1-300x150.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/MobileAppTesting-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/testlink-e1680261675504-1.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/TestRail-e1680261609742-1.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Travel-1.jpg
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/What-is-Exploratory-Testing_-1-1-1024x419.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/What-is-Exploratory-Testing_-1-1-300x123.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/What-is-Exploratory-Testing_-1-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/03/why-work-here-2.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/04/Cyber_Security-1-e1730117952973-300x195.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/04/Cyber_Security-1-e1730117952973-640x364.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/04/Cyber_Security-1-e1730117952973.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/04/Digital-Assurance-e1682654035504-1-150x150.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/2023/04/Digital-Assurance-e1682654035504-1-300x300.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/04/Digital-Assurance-e1682654035504-1-320x320.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/04/Digital-Assurance-e1682654035504-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/05/Engineering-Home-1-1-300x200.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/05/Engineering-Home-1-1.jpg
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/05/Services_banner_QE-e1684337302375-1-1024x353.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/05/Services_banner_QE-e1684337302375-1-300x103.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/05/Services_banner_QE-e1684337302375-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/06/Customer-Satisfaction-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/06/Security-Testing-Services-1-e1731289538553.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate002-e1690716237786-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate004-1-e1727692153719-300x158.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate004-1-e1727692153719.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate005-e1690732096817-1-300x153.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate005-e1690732096817-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/07/VST-Home-0005-2-1-150x150.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/07/VST-Home-0005-2-1-300x300.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/07/VST-Home-0005-2-1-320x320.jpg
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2023/07/VST-Home-0005-2-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/A-20-1-e1730195345387-223x300.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/A-20-1-e1730195345387.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/badge2.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-1024x433.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-1536x650.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-2048x867.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-300x127.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-768x325.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/E-commerce-and-Retail-e1730958682357.webp
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/EDTech-e1730958663954.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/2024/10/img-2@2x-1-248x300.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/img-2@2x-1-847x1024.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/img-2@2x-1.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/IoT-and-Smart-Devices-e1730958550602.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Media-and-Entertainment-e1730958634556.webp
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-18-at-3.22.07-PM-e1729764887836.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-18-at-3.22.10-PM-e1729764869724.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-23-at-12.21.03-PM.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-24-at-13.11.54-5-e1729764673300.jpeg
Method	GET
Parameter	x-content-type-options

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-24-at-3.27.27-PM-1-e1729764734764.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-24-at-3.27.28-PM-3.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.23.26.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.24.25.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.30.16.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.31.29.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.32.05.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.47.28.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-29-at-16.22.27.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-1024x495.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-1536x742.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-2048x989.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-300x145.jpeg
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-480x300.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-640x364.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-720x510.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/AccelESG-logo.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Advisory-Transformationv03-e1731289439749.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/ATLAS-Banner-480x300.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/ATLAS-Banner-640x350.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/2024/11/ATLAS-Banner-720x350.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/berribot-logo.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/CTE.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/HackerEarth-Logo.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-1024x549.jpeg

Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-300x161.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-480x300.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-640x364.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-720x510.jpeg

Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/kagoollogo.svg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Leanpitch-1.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/octalFrames_logo.png
Method	GET
Parameter	x-content-type-options

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02-1024x418.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02-1536x627.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02-2048x837.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02-300x123.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/preferredhcny-logo.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/PXL_20241030_110509234.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/PXL_20241030_124938251.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/2024/11/rollick-logo.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/seller-legend-300x45-1.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Test-Automationv002-300x210.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Test-Automationv002.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/the-credit-pros--300x34.png
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/the-credit-pros-.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Unocoin-logo-1.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VSoft-Logo-300x102.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VSoft-Logo.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-Culture-and-Values-300x185.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-Culture-and-Values.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home001.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home002.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home003.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home1.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home2.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home3.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/11/westoninfosec-1.png
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/12/Carees_VSt_003.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/12/software-testing_advisory_007.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/12/software-testing_cs_006.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/12/software-testing_QE_005.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/12/VST_Home_001.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/12/VST_Home_002.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2024/12/WhatsApp-Image-2024-11-28-at-16.12.24.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2025/01/IMG_20250106_164122-e1737460521938.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/2025/01/IMG_20250106_184150-e1737460619584.jpg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2025/04/CS_Service_01.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01-1024x465.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01-1536x698.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01-2048x931.jpeg
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01-300x136.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01.jpeg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/css/custom-apple-webkit.min.css?ver=1744173930
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/css/custom-frontend.min.css?ver=1744173930
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/inter.css?ver=1743442410
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/opensans.css?ver=1743442392
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/poppins.css?ver=1743442395
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/roboto.css?ver=1743442383
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/robotocondensed.css?ver=1744093863
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l0uumjng.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l1uumjng.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l2uumjng.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l3uumjng.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l5uum.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l6uumjng.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l9uumjng.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia0zl7suc.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia1pl7suc.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia1zl7.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia25l7suc.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia2jl7suc.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia2pl7suc.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia2zl7suc.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqw106f15m.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwt06f15m.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwte6f15m.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwtk6f15m.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwtu6f15m.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwu06f15m.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwuk6f15m.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwuu6f.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwvu6f15m.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwxu6f15m.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovts-muw.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovts2mu1ab.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtscmu1ab.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtsgmu1ab.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtskmu1ab.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtsomu1ab.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtsumu1ab.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtsymu1ab.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtugmu1ab.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtvomu1ab.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxiayp8kv8jhgfvrjjlme0tcmpi.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxiayp8kv8jhgfvrjjlme0tmmpkzsq.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlbt5z1jlfc-k.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlbt5z1xlfq.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlcz7z1jlfc-k.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlcz7z1xlfq.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrldd4z1jlfc-k.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrldd4z1xlfq.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrldz8z1jlfc-k.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrldz8z1xlfq.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlej6z1jlfc-k.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlej6z1xlfq.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlfj_z1jlfc-k.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlfj_z1xlfq.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlgt9z1jlfc-k.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlgt9z1xlfq.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm111vf9eo.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm111vgdeoceg.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm21lvf9eo.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm21lvgdeoceg.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm81xvf9eo.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm81xvgdeoceg.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmg1hvf9eo.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmg1hvgdeoceg.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmr19vf9eo.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmr19vgdeoceg.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmv1pvf9eo.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmv1pvgdeoceg.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmy15vf9eo.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmy15vgdeoceg.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxieyp8kv8jhgfvrjjfecg.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxieyp8kv8jhgfvrjjnecmne.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrjjluchta.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrjjlufntakpy.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrlptuchta.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrlptufntakpy.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkahkawzu.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkankawzu.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkbnka.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkbxkawzu.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkc3kawzu.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkchkawzu.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkcnkawzu.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkcxkawzu.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkenkawzu.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3-ubgee.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3cubgee.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3gubgee.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3iubgee.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3kubgee.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3oubgee.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3yuba.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluamawcubgee.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluamaxkubgee.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19elaam9uvi.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19elagm9uvi.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19elaqm9uvi.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19elawm9uvi.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19elcwm9uvi.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19eldam9uvi.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5jzbjeets9weq8-19eldwm9.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-19-7drs5.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-1927drs5.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-1967drs5.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-19a7drs5.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-19g7drs5.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-19k7dq.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-19y7drs5.woff2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/css/buttons.min.css?ver=6.7.2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/css/dashicons.min.css?ver=6.7.2

Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/css/dist/block-library/style.min.css?ver=6.7.2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/js/clipboard.min.js?ver=2.0.11
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/js/comment-reply.min.js?ver=6.7.2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/js/dist/a11y.min.js?ver=3156534cc54473497e14
Method	GET
Parameter	x-content-type-options
Attack	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/js/dist/dom-ready.min.js?ver=f77871ff7694fffea381
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/js/dist/hooks.min.js?ver=4d63a3d491d11ffd8ac6
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/js/dist/i18n.min.js?ver=5e580eb46a90c2b997e6
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/js/imagesloaded.min.js?ver=5.0.0
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/js/jquery/ui/core.min.js?ver=1.13.3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/wp-includes/js/underscore.min.js?ver=1.13.7
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/js/wp-util.min.js?ver=6.7.2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-includes/js/zxcvbn-async.min.js?ver=1.0
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-login.php
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	x-content-type-options
Attack	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/contact/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/penetration-testing/
Method	POST

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

Instances	529
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

INFORMATIONAL	CHARSET MISMATCH
Description	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set. An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dfooter
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dvst-main-footer
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dheader
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dnew-header
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dvst-main-header
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dcs-menu
Method	GET
Parameter	
Attack	

Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Delementor-1025
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dis-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dmenu-cybersecurity
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dqe-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservice-offerings

Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservices
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dtaas-menu
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fabout%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fai-driven-test-automation-2%2F
Method	GET
Parameter	
Attack	
Evidence	

Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fatlas%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fbest-practices-for-effective-software-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fblogs%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcareers%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcontact%2F
Method	GET

Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-performance-testing-and-monitoring%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Findustries%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2F
Method	GET
Parameter	
Attack	
Evidence	

Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Faccessibility-usability-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fadvisory-and-transformation%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fagile-and-devops-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fai-driven-test-automation%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-security-testing%2F
Method	GET

Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-testing-services%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fbusiness-experience-validation%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-native-application-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcompliance-and-security-audits%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcomprehensive-test-automation-framework%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcontinuous-quality-engineering%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcyber-resilience-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdata-driven-testing%2F
Method	GET
Parameter	

Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdevsecops-integration%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-and-embedded-systems-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanaged-soc-services%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanual-testing-services%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmobile-security-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fpenetration-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fperformance-engineering-monitoring%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fsecure-code-validation%2F
Method	GET
Parameter	
Attack	

Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fshift-left-and-shift-right-testing%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Ftest-center-of-excellence%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fvulnerability-assessment%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fzero-trust-network-assessments%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Futilizing-mobile-technology-in-the-field%2F

Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fvulnerability-assessments-penetration-testing-cybersecurity%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-exploratory-testing-why-and-when-do-we-need-it%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-integration-testing-and-types-approach%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhy-cloud-security-testing-is-essential%2F
Method	GET
Parameter	
Attack	

Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhy-do-the-mobile-manual-test%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhy-is-independent-software-testing-vital-to-successful-applications-in-any-industry%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
Instances	59
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011

INFORMATIONAL	INFORMATION DISCLOSURE - SUSPICIOUS COMMENTS
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://virtuestech.com
Method	GET
Parameter	
Attack	

Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/cdn-cgi/scripts/7d0fa10a/cloudflare-static/rocket-loader.min.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//www.w3.org/2000/svg",E={"application/ecmascript":!0,"application/javascript":!0,"application/x-ecmascript":!0,"application/x-j", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/contact/
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	
Attack	
Evidence	user

Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/
Method	GET
Parameter	
Attack	
Evidence	From
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	
Attack	
Evidence	User
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	
Attack	
Evidence	Where
Other Info	The following pattern was used: \bWHERE\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.

URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	
Attack	
Evidence	From
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	
Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	

Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	
Attack	
Evidence	user

Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/includes/js/index.js?ver=6.0.5
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//,""),o=r?n+"/"+r:n),"string"==typeof o&&(-1!==t.indexOf("?")&&(o=o.replace("?","&")),o=o.replace(/^\//,""),c=t+o),i={Accept:"a", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//www.youtube-nocookie.com",s.origin=window.location.hostname),n.addClass("elementor-loading elementor-invisible"),this.player=n", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/js/rbtools.min.js?ver=6.7.19
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//greensock.com",!v.nullTargetWarn)||[],u._ptLookup=[],u._overwrite=C,F||w||B(_)||B(y)){if(n=u.vars,(l=u.timeline=new Me({data:"", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/js/rs6.min.js?ver=6.7.19
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//")?"http://":0===e.url.indexOf("https://")?"https://":0===e.url.indexOf("//")?"//":"relative";var t=e.url.replace("https://","", see evidence field for the suspicious comment/snippet.

URL	https://virtuestech.com/wp-content/themes/hub/assets/js/theme.min.js
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//www.w3.org/2000/svg" width="150" height="152" viewBox="-2 0 154 150" class="w-100 h-100 w-full h-full"><circle fill="none" cx=", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/bootstrap/js/bootstrap.min.js
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//popper.js.org)"); let t = this._element; "parent" === this._config.reference ? t = this._parent : o(this._config.reference)", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/flickity/flickity.pkgd.min.js
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//bit.ly/getsizebug1")}return e}var n=false;var C;function x(){if(n){return}n=true;var t=document.createElement("div");t.style.w", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/gsap/minified/gsap.min.js
Method	GET
Parameter	
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected in likely comment: "//gsap.com",!q.nullTargetWarn)|| [],a._ptLookup=[],a._overwrite=b,x||T||y(_)||y(m)){if(r=a.vars,(s=a.timeline=new Xt({data:"neste", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/isotope/isotope.pkgd.min.js
Method	GET
Parameter	

Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//bit.ly/getsizebug1")}return e}var n=false;var S;function b(){if(n){return}n=true;var t=document.createElement("div");t.style.w", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//github.com/zloirock/core-js/blob/v3.35.1/LICENSE",source:"https://github.com/zloirock/core-js"})},function(r,t,e){r.exports=!1", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
Method	GET
Parameter	
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://virtuestech.com/wp-login.php
Method	GET
Parameter	
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in likely comment: "//virtuestech.com/wp-admin/js/password-strength-meter.min.js?ver=6.7.2" id="password-strength-meter-js"></script>", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	
Attack	
Evidence	admin

Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in likely comment: "//virtuestech.com/wp-admin/js/password-strength-meter.min.js?ver=6.7.2" id="password-strength-meter-js"> </script>", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/
Method	POST
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/contact/
Method	POST
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	
Attack	
Evidence	User
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.

URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	
Attack	
Evidence	Where
Other Info	The following pattern was used: \bWHERE\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	
Attack	
Evidence	From
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	
Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/penetration-testing/
Method	POST

Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//schema.org","@graph":[{"@type":["ProfessionalService","Organization"],"@id":"https://virtuestech.com/#organization","name":"Vi", see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in likely comment: "//virtuestech.com/wp-admin/js/password-strength-meter.min.js?ver=6.7.2" id="password-strength-meter-js"> </script>", see evidence field for the suspicious comment/snippet.
Instances	43
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://virtuestech.com
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	
Attack	

Evidence	<a class="elementor-icon elementor-social-icon elementor-social-icon-facebook-square elementor-repeater-item-7ab750c" target="_blank"> Facebook-square <svg class="e-font-icon-svg e-fab-facebook-square" viewBox="0 0 448 512" xmlns="http://www.w3.org/2000/svg"> <path d="M400 32H48A48 48 0 0 0 0 80v352a48 48 0 0 0 48 48h137.25V327.69h-63V256h63v-54.64c0-62.15 37-96.48 93.67-96.48 27.14 0 55.52 4.84 55.52 4.84v61h-31.27c-30.81 0-40.42 19.12-40.42 38.73V256h68.78l-11 71.69h-57.78V480H400a48 48 0 0 0 48-48V80a48 48 0 0 0-48-48z"></path></svg> </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://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	
Attack	
Evidence	<a class="elementor-icon elementor-social-icon elementor-social-icon-facebook elementor-repeater-item-ffab50c" target="_blank"> Facebook <svg class="e-font-icon-svg e-fab-facebook" viewBox="0 0 512 512" xmlns="http://www.w3.org/2000/svg"><path d="M504 256C504 119 393 8 256 8S8 119 8 256c0 123.78 90.69 226.38 209.25 245V327.69h-63V256h63v-54.64c0-62.15 37-96.48 93.67-96.48 27.14 0 55.52 4.84 55.52 4.84v61h-31.28c-30.8 0-40.41 19.12-40.41 38.73V256h68.78l-11 71.69h-57.78V501C413.31 482.38 504 379.78 504 256z"></path></svg> </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://virtuestech.com/?liquid-header=header
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	
Attack	

Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	
Attack	
Evidence	<a class="elementor-button btn btn-naked btn-icon-right btn-hover-reveal btn-has-label" > Proactive Defense for a Resilient Digital Future </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://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	
Attack	
Evidence	<a href="#"class="elementor-button btn btn-naked btn-icon-right btn-hover-reveal btn-has-label" > Quality Assurance </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://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	
Attack	
Evidence	<a class="elementor-button btn btn-naked btn-icon-shaped btn-has-label" > Future-Ready Strategies for Unmatched Growth </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://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	
Attack	
Evidence	<a href="#"class="elementor-button btn btn-naked btn-icon-right btn-hover-reveal btn-has-label" > Security advisory </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://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	
Attack	
Evidence	<a class="elementor-button btn btn-naked btn-icon-shaped btn-has-label" > Empower Your Digital Transformation with Flawless Quality </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://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	
Attack	
Evidence	<a href="https://virtuestech.com/ai-driven-test-automation/" class="lqd-overlay z-index-2" target="_self" aria-label="AI driven Test Automation "></a>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
URL	https://virtuestech.com/?liquid-mega-menu=services

Method	GET
Parameter	
Attack	
Evidence	<a href="#"class="elementor-button btn btn-naked btn-icon-right btn-hover-reveal btn-has-label" > Quality Engineering </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://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	
Attack	
Evidence	<a href="#"class="elementor-button btn btn-naked btn-icon-right btn-hover-reveal btn-has-label" > Talent as a service </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://virtuestech.com/?page_id=20760
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/about/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/advisorytransformation
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/atlas/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/author/virtuestech/

Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/blogs/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/careers/
Method	GET
Parameter	
Attack	

Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/category/cyber-security/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	
Attack	

Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/category/software-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/category/uncategorized/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/contact/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/cybersecurity-services/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/industries/

Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/insights/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/services/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	
Attack	

Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/ai-driven-test-automation/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/cloud-native-application-testing/

Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	
Attack	

Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/devsecops-integration/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/managed-soc-services/

Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	
Attack	

Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/performance-testing-services
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/security-audits-and-compliance
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/vulnerability-assessment/

Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/tag/automation-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"> </path></svg></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://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	
Attack	

Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/tag/software-testing/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/tag/test-automation/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/what-is-integration-testing-and-types-approach/

Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	
Attack	

Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png
Method	GET
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/atlas/

Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/contact/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	
Attack	

Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/cloud-security-testing/

Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	
Attack	

Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/manual-testing-services/

Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	
Attack	

Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	
Attack	
Evidence	<a>Quality Engineering<svg xmlns="http://www.w3.org/2000/svg" width="21" height="32" viewBox="0 0 21 32" style="width: 1em; height: 1em;"><path fill="currentColor" d="M10.5 18.375l7.938-7.938c.562-.562 1.562-.562 2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.5.625-2.063.062L.437 12.562C.126 12.25 0 11.876 0 11.5s.125-.75.438-1.063c.562-.562 1.562-.562 2.124 0z"></path></svg></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	112
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://virtuestech.com
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-footer=vst-main-footer
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	cache-control
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/about/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/about/embed/
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/ai-driven-test-automation-2/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/atlas/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/atlas/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/author/virtuestech/
Method	GET
Parameter	cache-control
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/author/virtuestech/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/best-practices-for-effective-software-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/best-practices-for-effective-software-testing/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/best-practices-for-effective-software-testing/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/blogs/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/blogs/embed/
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/blogs/page/2/?ajaxify=1
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/careers/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/careers/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/cyber-security/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/cyber-security/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/category/digital-assurance/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/digital-assurance/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/quality-engineering/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/quality-engineering/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/software-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/software-testing/feed/
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/uncategorized/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/category/uncategorized/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/comments/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/contact/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/contact/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/feed/
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/industries/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/industries/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/robots.txt
Method	GET
Parameter	cache-control
Attack	
Evidence	max-age=14400
Other Info	
URL	https://virtuestech.com/services/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	GET
Parameter	cache-control
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/accessibility-usability-testing/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/advisory-and-transformation/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/agile-and-devops-testing/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/ai-driven-test-automation/

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/ai-driven-test-automation/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-security-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-security-testing/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-testing-services/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/api-testing-services/embed/
Method	GET
Parameter	cache-control
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/business-experience-validation/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/business-experience-validation/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-native-application-testing/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cloud-security-testing/embed/

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/compliance-and-security-audits/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	GET
Parameter	cache-control
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/continuous-quality-engineering/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/cyber-resilience-testing/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/data-driven-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/data-driven-testing/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/devsecops-integration/

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/devsecops-integration/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-security-testing/
Method	GET
Parameter	cache-control
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/iot-security-testing/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/penetration-testing/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/embed/
Method	GET
Parameter	cache-control
Attack	

Evidence	
Other Info	
URL	https://virtuestech.com/services/secure-code-validation/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/secure-code-validation/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/services/test-center-of-excellence/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/vulnerability-assessment/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/services/zero-trust-network-assessments/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/automation-testing/
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/automation-testing/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/integration-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/integration-testing/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/manual-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/manual-testing/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/tag/software-testing/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/software-testing/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/test-automation/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/tag/test-automation/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/utilizing-mobile-technology-in-the-field/embed/
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/feed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/what-is-integration-testing-and-types-approach/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-cloud-security-testing-is-essential/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-do-the-mobile-manual-test/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-do-the-mobile-manual-test/embed/
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry/embed/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dfooter
Method	GET
Parameter	cache-control

Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dvst-main-footer
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dheader
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dnew-header
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dvst-main-header
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dcs-menu
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Delementor-1025
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dis-menu
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dmenu-cybersecurity
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dqe-menu
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservice-offerings
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservices
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dtaas-menu
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fabout%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fai-driven-test-automation-2%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fatlas%2F
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fbest-practices-for-effective-software-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fblogs%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcareers%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcontact%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry%2F

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-performance-testing-and-monitoring%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Findustries%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Faccessibility-usability-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fadvisory-and-transformation%2F

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fagile-and-devops-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fai-driven-test-automation%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-security-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-testing-services%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fbusiness-experience-validation%2F

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-native-application-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-security-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcompliance-and-security-audits%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcomprehensive-test-automation-framework%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcontinuous-quality-engineering%2F

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcyber-resilience-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdata-driven-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdevsecops-integration%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-and-embedded-systems-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-security-testing%2F

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanaged-soc-services%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanual-testing-services%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmobile-security-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fpenetration-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fperformance-engineering-monitoring%2F

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fsecure-code-validation%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fshift-left-and-shift-right-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Ftest-center-of-excellence%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fvulnerability-assessment%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fzero-trust-network-assessments%2F

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Futilizing-mobile-technology-in-the-field%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fvulnerability-assessments-penetration-testing-cybersecurity%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-exploratory-testing-why-and-when-do-we-need-it%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-integration-testing-and-types-approach%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhy-cloud-security-testing-is-essential%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhy-do-the-mobile-manual-test%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fwhy-is-independent-software-testing-vital-to-successful-applications-in-any-industry%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dfooter
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-footer%3Dvst-main-footer
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dheader
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dnew-header
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-header%3Dvst-main-header
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dcs-menu
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Delementor-1025
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dis-menu
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dmenu-cybersecurity
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dqe-menu
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservice-offerings
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dservices
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquid-mega-menu%3Dtaas-menu
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fabout%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fai-driven-test-automation-2%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fatlas%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	

URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fbest-practices-for-effective-software-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fblogs%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fcareers%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fcontact%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fimportance-of-performance-testing-and-monitoring%2F

Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Findustries%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Faccessibility-usability-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fadvisory-and-transformation%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fagile-and-devops-testing%2F
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fai-driven-test-automation%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-security-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fapi-testing-services%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fbusiness-experience-validation%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-native-application-testing%2F
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcloud-security-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcompliance-and-security-audits%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcomprehensive-test-automation-framework%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcontinuous-quality-engineering%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcyber-resilience-testing%2F
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdata-driven-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fdevsecops-integration%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-and-embedded-systems-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fiot-security-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanaged-soc-services%2F
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmanual-testing-services%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fmobile-security-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fpenetration-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fperformance-engineering-monitoring%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fsecure-code-validation%2F
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fshift-left-and-shift-right-testing%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Ftest-center-of-excellence%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fvulnerability-assessment%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fzero-trust-network-assessments%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Futilizing-mobile-technology-in-the-field%2F
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fvulnerability-assessments-penetration-testing-cybersecurity%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-exploratory-testing-why-and-when-do-we-need-it%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhat-is-integration-testing-and-types-approach%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhy-cloud-security-testing-is-essential%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhy-do-the-mobile-manual-test%2F
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fwhy-is-independent-software-testing-vital-to-successful-applications-in-any-industry%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/categories/1
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/categories/30
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/categories/34
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/categories/35
Method	GET
Parameter	cache-control
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/categories/36
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/13610
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/13621
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/13645
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/13749
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/14364
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/14382
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/188
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/19359
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/19466
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/19537
Method	GET
Parameter	cache-control
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20009
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20587
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20606
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20670
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20732
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20738
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20754
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/20790
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/21974
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22561
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22566
Method	GET
Parameter	cache-control
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22571
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22576
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22581
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22586
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22591
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22675
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22680
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22685
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22690
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22695
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22700
Method	GET
Parameter	cache-control
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22708
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/22906
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/256
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/pages/271
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13377
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13410
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13420
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13428
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/13434
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/15119
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/21232
Method	GET
Parameter	cache-control
Attack	
Evidence	

Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/21263
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/22176
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/posts/3500
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/28
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/29
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/31
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/32
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/tags/33
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-json/wp/v2/users/1
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-login.php
Method	GET
Parameter	cache-control
Attack	
Evidence	no-cache, must-revalidate, max-age=0
Other Info	
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET
Parameter	cache-control
Attack	

Evidence	no-cache, must-revalidate, max-age=0
Other Info	
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	cache-control
Attack	
Evidence	no-cache, must-revalidate, max-age=0
Other Info	
Instances	313
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/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

INFORMATIONAL	RETRIEVED FROM CACHE
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://virtuestech.com/wp-admin/css/forms.min.css?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	Age: 168229
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-admin/css/login.min.css?ver=6.7.2

Method	GET
Parameter	
Attack	
Evidence	Age: 168229
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-admin/js/password-strength-meter.min.js?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	Age: 420004
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-admin/js/user-profile.min.js?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	Age: 420004
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=6.0.5
Method	GET
Parameter	
Attack	
Evidence	Age: 249084
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/includes/js/index.js?ver=6.0.5
Method	GET
Parameter	
Attack	
Evidence	Age: 597321
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/includes/sw/js/index.js?ver=6.0.5
Method	GET

Parameter	
Attack	
Evidence	Age: 369880
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/modules/recaptcha/index.js?ver=6.0.5
Method	GET
Parameter	
Attack	
Evidence	Age: 186789
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/css/widget-divider.min.css?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	Age: 186789
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/css/widget-image.min.css?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	Age: 168217
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/css/widget-social-icons.min.css?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	Age: 186789
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/css/widget-spacer.min.css?ver=3.28.3
Method	GET
Parameter	

Attack	
Evidence	Age: 173857
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/js/frontend-modules.min.js?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	Age: 186789
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	Age: 186789
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	Age: 186789
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/all.min.css?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	Age: 186788
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/v4-shims.min.css?ver=3.28.3
Method	GET
Parameter	
Attack	

Evidence	Age: 186788
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/elementor/assets/lib/font-awesome/js/v4-shims.min.js?ver=3.28.3
Method	GET
Parameter	
Attack	
Evidence	Age: 3766
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/hub-elementor-addons/assets/css/blog/blog-single/blog-single-base.css?ver=5.0.7
Method	GET
Parameter	
Attack	
Evidence	Age: 419987
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/hub-elementor-addons/assets/css/pages/not-found.css?ver=5.0.7
Method	GET
Parameter	
Attack	
Evidence	Age: 419994
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/hub-elementor-addons/assets/css/theme-elementor.min.css?ver=5.0.7
Method	GET
Parameter	
Attack	
Evidence	Age: 535004
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/assets/dummy.png
Method	GET
Parameter	
Attack	

Evidence	Age: 531024
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/css/rs6.css?ver=6.7.19
Method	GET
Parameter	
Attack	
Evidence	Age: 597321
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/js/rbtools.min.js?ver=6.7.19
Method	GET
Parameter	
Attack	
Evidence	Age: 597321
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/plugins/revslider/sr6/assets/js/rs6.min.js?ver=6.7.19
Method	GET
Parameter	
Attack	
Evidence	Age: 455154
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/js/theme.min.js
Method	GET
Parameter	
Attack	
Evidence	Age: 369880
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/bootstrap/css/bootstrap.min.css
Method	GET
Parameter	
Attack	

Evidence	Age: 597320
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/bootstrap/js/bootstrap.min.js
Method	GET
Parameter	
Attack	
Evidence	Age: 369880
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/fastdom/fastdom.min.js
Method	GET
Parameter	
Attack	
Evidence	Age: 531018
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/flickity/flickity-fade.min.js
Method	GET
Parameter	
Attack	
Evidence	Age: 594965
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/flickity/flickity.pkgd.min.js
Method	GET
Parameter	
Attack	
Evidence	Age: 367283
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/fontfaceobserver.js
Method	GET
Parameter	
Attack	
Evidence	Age: 597321

Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/fresco/css/fresco.css
Method	GET
Parameter	
Attack	
Evidence	Age: 369880
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/fresco/js/fresco.js
Method	GET
Parameter	
Attack	
Evidence	Age: 168225
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/gsap/minified/gsap.min.js
Method	GET
Parameter	
Attack	
Evidence	Age: 597321
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/gsap/utils/SplitText.min.js
Method	GET
Parameter	
Attack	
Evidence	Age: 369880
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/intersection-observer.js
Method	GET
Parameter	
Attack	
Evidence	Age: 597321

Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/isotope/isotope.pkgd.min.js
Method	GET
Parameter	
Attack	
Evidence	Age: 531020
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/isotope/packery-mode.pkgd.min.js
Method	GET
Parameter	
Attack	
Evidence	Age: 531020
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/jquery-ui/jquery-ui.min.js
Method	GET
Parameter	
Attack	
Evidence	Age: 455154
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/lazyload.min.js
Method	GET
Parameter	
Attack	
Evidence	Age: 597321
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/liquid-icon/lqd-essentials/fonts/lqd-essentials.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 457684

Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/liquid-icon/lqd-essentials/lqd-essentials.min.css
Method	GET
Parameter	
Attack	
Evidence	Age: 531018
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/lity/lity.min.js
Method	GET
Parameter	
Attack	
Evidence	Age: 597321
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/themes/hub/assets/vendors/tinycolor-min.js
Method	GET
Parameter	
Attack	
Evidence	Age: 531018
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-icon-1.svg
Method	GET
Parameter	
Attack	
Evidence	Age: 320943
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1-1024x276.png
Method	GET
Parameter	
Attack	
Evidence	Age: 419998

Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1-1536x414.png
Method	GET
Parameter	
Attack	
Evidence	Age: 193521
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1-2048x552.png
Method	GET
Parameter	
Attack	
Evidence	Age: 419998
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1-300x81.png
Method	GET
Parameter	
Attack	
Evidence	Age: 168224
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech-VST-1.png
Method	GET
Parameter	
Attack	
Evidence	Age: 491698
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/08/VirtuesTech_LOGO-1.png
Method	GET
Parameter	
Attack	
Evidence	Age: 419985
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL	https://virtuestech.com/wp-content/uploads/2021/10/Integration-testing-1-300x150.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419991
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Integration-testing-1-640x350.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 584428
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Integration-testing-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 512503
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/10/software-testing-trends-1-300x150.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419987
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/10/software-testing-trends-1-640x364.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 379353
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/10/software-testing-trends-1-720x400.jpg

Method	GET
Parameter	
Attack	
Evidence	Age: 532616
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/10/software-testing-trends-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 526987
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues-e1678973425717-1-300x173.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193521
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues-e1678973425717-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 110208
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1665455409401-1024x791.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 168215
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1665455409401.jpg
Method	GET

Parameter	
Attack	
Evidence	Age: 592773
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer.png
Method	GET
Parameter	
Attack	
Evidence	Age: 80093
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1-150x150.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 423524
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1-300x300.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193522
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1-320x320.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193522
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1-760x760.jpg
Method	GET
Parameter	

Attack	
Evidence	Age: 168219
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Automation-Services-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419993
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/bugzilla-e1680261726322-1.png
Method	GET
Parameter	
Attack	
Evidence	Age: 419998
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1-300x150.png
Method	GET
Parameter	
Attack	
Evidence	Age: 193522
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1-480x300.png
Method	GET
Parameter	
Attack	
Evidence	Age: 168208
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1-640x364.png
Method	GET
Parameter	
Attack	

Evidence	Age: 320947
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Data-loss-prevention-1-720x450.png
Method	GET
Parameter	
Attack	
Evidence	Age: 436782
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Energy-Utilities-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 9724
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Financial-Services-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 367267
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Healthcare-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 375274
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/HP-Quality-Center-e1680262577123-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 533111

Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Independent-Quality-Assurance-Testing-1-300x150.png
Method	GET
Parameter	
Attack	
Evidence	Age: 419986
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Independent-Quality-Assurance-Testing-1.png
Method	GET
Parameter	
Attack	
Evidence	Age: 526986
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Jira-e1680262548454-1.png
Method	GET
Parameter	
Attack	
Evidence	Age: 533111
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/MantisBT-Logo-1-e1680262729435-1.webp
Method	GET
Parameter	
Attack	
Evidence	Age: 391870
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Mobile-app-test-1-150x150.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 423507
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL	https://virtuestech.com/wp-content/uploads/2023/03/Mobile-app-test-1-300x300.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 193520
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Mobile-app-test-1-320x320.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 420005
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Mobile-app-test-1.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 401093
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/MobileAppTesting-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 445564
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/testlink-e1680261675504-1.png
Method	GET
Parameter	
Attack	
Evidence	Age: 533111
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/TestRail-e1680261609742-1.png

Method	GET
Parameter	
Attack	
Evidence	Age: 533110
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/Travel-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 4525
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/What-is-Exploratory-Testing_-1-1-1024x419.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419988
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/What-is-Exploratory-Testing_-1-1-300x123.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193523
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/What-is-Exploratory-Testing_-1-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193524
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/03/why-work-here-2.jpg
Method	GET

Parameter	
Attack	
Evidence	Age: 379367
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/04/Cyber_Security-1-e1730117952973-300x195.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193524
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/04/Cyber_Security-1-e1730117952973-640x364.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 379354
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/04/Cyber_Security-1-e1730117952973.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 9726
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/04/Digital-Assurance-e1682654035504-1-150x150.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193525
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/04/Digital-Assurance-e1682654035504-1-300x300.jpg
Method	GET
Parameter	

Attack	
Evidence	Age: 193525
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/04/Digital-Assurance-e1682654035504-1-320x320.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 168233
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/04/Digital-Assurance-e1682654035504-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 168230
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/05/Engineering-Home-1-1-300x200.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193523
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/05/Engineering-Home-1-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193519
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/05/Services_banner_QE-e1684337302375-1-1024x353.jpg
Method	GET
Parameter	
Attack	

Evidence	Age: 419983
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/05/Services_banner_QE-e1684337302375-1-300x103.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419984
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/05/Services_banner_QE-e1684337302375-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419984
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/06/Customer-Satisfaction-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 591324
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/06/Security-Testing-Services-1-e1731289538553.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419998
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate002-e1690716237786-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 423328

Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate004-1-e1727692153719-300x158.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193523
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate004-1-e1727692153719.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 423362
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/07/Accelerate005-e1690732096817-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419990
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/07/VST-Home-0005-2-1-300x300.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193519
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2023/07/VST-Home-0005-2-1-320x320.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419985
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL	https://virtuestech.com/wp-content/uploads/2023/07/VST-Home-0005-2-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 535387
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/A-20-1-e1730195345387-223x300.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193520
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/A-20-1-e1730195345387.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 518935
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/badge2.png
Method	GET
Parameter	
Attack	
Evidence	Age: 456478
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-1024x433.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419997
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-1536x650.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419997
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-300x127.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419997
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-768x325.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419997
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 426440
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/E-commerce-and-Retail-e1730958682357.webp
Method	GET
Parameter	
Attack	
Evidence	Age: 323314

Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/EDTech-e1730958663954.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 9724
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/img-2@2x-1.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 369873
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/IoT-and-Smart-Devices-e1730958550602.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 9724
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Media-and-Entertainment-e1730958634556.webp
Method	GET
Parameter	
Attack	
Evidence	Age: 9724
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-18-at-3.22.07-PM-e1729764887836.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 546892

Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-18-at-3.22.10-PM-e1729764869724.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 591323
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-23-at-12.21.03-PM.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 391856
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-24-at-13.11.54-5-e1729764673300.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 591323
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-24-at-3.27.27-PM-1-e1729764734764.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 591324
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.23.26.jpeg
Method	GET
Parameter	
Attack	

Evidence	Age: 391856
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.24.25.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 456478
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.30.16.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 110094
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.31.29.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 546892
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.32.05.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 591323
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-25-at-11.47.28.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 591323

Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/WhatsApp-Image-2024-10-29-at-16.22.27.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 535387
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-1024x495.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 419988
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-1536x742.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 419988
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-2048x989.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 419988
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-300x145.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 419988
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-480x300.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 473031
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-640x364.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 584429
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical-720x510.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 86147
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/10/Why-Regular-VAPT-Are-Critical.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 426440
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/AccelESG-logo.png
Method	GET
Parameter	
Attack	
Evidence	Age: 249063
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Advisory-Transformationv03-e1731289439749.jpg

Method	GET
Parameter	
Attack	
Evidence	Age: 286278
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/ATLAS-Banner-480x300.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419988
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/ATLAS-Banner-640x350.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193519
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/ATLAS-Banner-720x350.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419995
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/berribot-logo.png
Method	GET
Parameter	
Attack	
Evidence	Age: 530999
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/CTE.jpg
Method	GET

Parameter	
Attack	
Evidence	Age: 531000
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/HackerEarth-Logo.png
Method	GET
Parameter	
Attack	
Evidence	Age: 438474
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-1024x549.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 419984
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-300x161.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 419984
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-480x300.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 9724
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-640x364.jpeg

Method	GET
Parameter	
Attack	
Evidence	Age: 419998
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-720x510.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 452196
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 372416
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/kagoollogo.svg
Method	GET
Parameter	
Attack	
Evidence	Age: 530999
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Leanpitch-1.png
Method	GET
Parameter	
Attack	
Evidence	Age: 530999
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/octalFrames_logo.png

Method	GET
Parameter	
Attack	
Evidence	Age: 530999
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02-1024x418.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 420002
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02-1536x627.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 420003
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02-2048x837.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 420003
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02-300x123.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 193521
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Performance-post_02.jpeg

Method	GET
Parameter	
Attack	
Evidence	Age: 379337
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/preferredhcny-logo.png
Method	GET
Parameter	
Attack	
Evidence	Age: 249063
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/PXL_20241030_110509234.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 546892
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/PXL_20241030_124938251.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 175389
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/rollick-logo.png
Method	GET
Parameter	
Attack	
Evidence	Age: 367265
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/seller-legend-300x45-1.png
Method	GET

Parameter	
Attack	
Evidence	Age: 530999
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Test-Automationv002-300x210.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419997
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Test-Automationv002.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193520
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/the-credit-pros--300x34.png
Method	GET
Parameter	
Attack	
Evidence	Age: 110905
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/the-credit-pros-.png
Method	GET
Parameter	
Attack	
Evidence	Age: 367287
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/Unocoin-logo-1.png
Method	GET
Parameter	

Attack	
Evidence	Age: 530999
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VSoft-Logo-300x102.png
Method	GET
Parameter	
Attack	
Evidence	Age: 531000
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VSoft-Logo.png
Method	GET
Parameter	
Attack	
Evidence	Age: 419974
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-Culture-and-Values-300x185.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 419993
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-Culture-and-Values.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 597314
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home001.png
Method	GET
Parameter	
Attack	

Evidence	Age: 419998
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home002.png
Method	GET
Parameter	
Attack	
Evidence	Age: 419998
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home003.png
Method	GET
Parameter	
Attack	
Evidence	Age: 419998
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home1.png
Method	GET
Parameter	
Attack	
Evidence	Age: 193520
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/VST-home3.png
Method	GET
Parameter	
Attack	
Evidence	Age: 419998
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/11/westoninfosec-1.png
Method	GET
Parameter	
Attack	
Evidence	Age: 438474

Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/12/Carees_VSt_003.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 9724
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/12/software-testing_advisory_007.png
Method	GET
Parameter	
Attack	
Evidence	Age: 367267
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/12/software-testing_cs_006.png
Method	GET
Parameter	
Attack	
Evidence	Age: 531000
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/12/software-testing_QE_005.png
Method	GET
Parameter	
Attack	
Evidence	Age: 367264
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/12/VST_Home_001.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193520
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL	https://virtuestech.com/wp-content/uploads/2024/12/VST_Home_002.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 193520
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2024/12/WhatsApp-Image-2024-11-28-at-16.12.24.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 591322
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2025/01/IMG_20250106_164122-e1737460521938.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 456477
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2025/01/IMG_20250106_184150-e1737460619584.jpg
Method	GET
Parameter	
Attack	
Evidence	Age: 546892
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2025/04/CS_Service_01.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 109223
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01-1024x465.jpeg

Method	GET
Parameter	
Attack	
Evidence	Age: 106832
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01-1536x698.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 107012
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01-2048x931.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 106832
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01-300x136.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 106832
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/2025/04/QE_Service_01.jpeg
Method	GET
Parameter	
Attack	
Evidence	Age: 109224
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/css/custom-apple-webkit.min.css?ver=1744173930
Method	GET

Parameter	
Attack	
Evidence	Age: 18654
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/css/custom-frontend.min.css?ver=1744173930
Method	GET
Parameter	
Attack	
Evidence	Age: 18654
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/inter.css?ver=1743442410
Method	GET
Parameter	
Attack	
Evidence	Age: 369880
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/opensans.css?ver=1743442392
Method	GET
Parameter	
Attack	
Evidence	Age: 103503
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/poppins.css?ver=1743442395
Method	GET
Parameter	
Attack	
Evidence	Age: 103504
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/roboto.css?ver=1743442383
Method	GET
Parameter	

Attack	
Evidence	Age: 103504
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/robotocondensed.css?ver=1744093863
Method	GET
Parameter	
Attack	
Evidence	Age: 102148
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l0uumjng.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420007
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l1uumjng.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 106823
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l3uumjng.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420007
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l5uum.woff2

Method	GET
Parameter	
Attack	
Evidence	Age: 535016
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l6uumjng.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 106823
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqg7ca725jhhknnqk6l9uumjng.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193523
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia0zl7suc.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420007
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia1pl7suc.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420007
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia1zl7.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193522
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia25l7suc.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193523
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia2jl7suc.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420008
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia2pl7suc.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193523
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmxcp50sjia2zl7suc.woff2
Method	GET
Parameter	
Attack	

Evidence	Age: 420007
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqw106f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420006
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwte6f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420005
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwtk6f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420005
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwtu6f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193521
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwuk6f15m.woff2
Method	GET

Parameter	
Attack	
Evidence	Age: 420005
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwvu6f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193521
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba-ufuicvxscekx2cmqvxlwqwxu6f15m.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420006
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovts-muw.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 168211
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovts2mu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420005
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtscmu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420005
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtsgmu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420005
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtskmu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420005
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtsomu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420005
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtsymu1ab.woff2
Method	GET
Parameter	
Attack	

Evidence	Age: 420006
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtugmu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193521
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba-uvwbx2vvnxbbobj2ovtvomu1ab.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193521
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxiayp8kv8jhgfvrjjlme0tcmpi.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420007
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxiayp8kv8jhgfvrjjlme0tmmpkzsq.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420007
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlbt5z1jlfc-k.woff2
Method	GET

Parameter	
Attack	
Evidence	Age: 420006
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlbt5z1xlfq.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193522
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlcz7z1jlfc-k.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193521
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlcz7z1xlfq.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193521
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrldd4z1jlfc-k.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193522
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrldd4z1xlfq.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193522
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrldz8z1xlfq.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 602980
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlej6z1jlfc-k.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420006
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlej6z1xlfq.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193522
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlfj_z1jlfc-k.woff2
Method	GET
Parameter	
Attack	

Evidence	Age: 193521
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlfj_z1xlfq.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420006
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlgt9z1jlfc-k.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193521
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm111vgdeoceg.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420006
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm21lvf9eo.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193522
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm81xvf9eo.woff2
Method	GET

Parameter	
Attack	
Evidence	Age: 420006
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlm81xvgdeoceg.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420007
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmg1hvf9eo.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420006
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmg1hvgdeoceg.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420007
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmr19vf9eo.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420007
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmr19vgdeoceg.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420007
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmv1pvf9eo.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420006
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmv1pvgdeoceg.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420007
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmy15vf9eo.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420006
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrjjlmy15vgdeoceg.woff2
Method	GET
Parameter	
Attack	

Evidence	Age: 193522
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxieyp8kv8jhgfvrjjnecmne.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193522
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrjjlufntakpy.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 106824
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrlptuchta.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420006
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrlptufntakpy.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 106824
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkankawzu.woff2
Method	GET

Parameter	
Attack	
Evidence	Age: 420011
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkbnka.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193527
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkbxkawzu.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193527
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkc3kawzu.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 168217
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkchkawzu.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420011
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkcnkawzu.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420012
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkcxkawzu.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420012
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec9_vu3r1gihoszmkenkawzu.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420011
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3-ubgee.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420012
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3cubgee.woff2
Method	GET
Parameter	
Attack	

Evidence	Age: 420011
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3gubgee.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420012
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3kubgee.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 168217
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3oubgee.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 420012
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluama3yuba.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193527
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluamawcubgee.woff2
Method	GET

Parameter	
Attack	
Evidence	Age: 193527
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn66agldtyluamaxkubgee.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 193527
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5jzbjeets9weq8-19k7dq.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 102163
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/css/buttons.min.css?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	Age: 420004
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/css/dashicons.min.css?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	Age: 420004
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/css/dist/block-library/style.min.css?ver=6.7.2
Method	GET

Parameter	
Attack	
Evidence	Age: 420006
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/clipboard.min.js?ver=2.0.11
Method	GET
Parameter	
Attack	
Evidence	Age: 423558
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/comment-reply.min.js?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	Age: 419984
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/dist/a11y.min.js?ver=3156534cc54473497e14
Method	GET
Parameter	
Attack	
Evidence	Age: 193525
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/dist/dom-ready.min.js?ver=f77871ff7694fffea381
Method	GET
Parameter	
Attack	
Evidence	Age: 420004
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/dist/hooks.min.js?ver=4d63a3d491d11ffd8ac6
Method	GET
Parameter	

Attack	
Evidence	Age: 531018
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/dist/i18n.min.js?ver=5e580eb46a90c2b997e6
Method	GET
Parameter	
Attack	
Evidence	Age: 597321
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
Method	GET
Parameter	
Attack	
Evidence	Age: 423562
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/imagesloaded.min.js?ver=5.0.0
Method	GET
Parameter	
Attack	
Evidence	Age: 369880
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1
Method	GET
Parameter	
Attack	
Evidence	Age: 369879
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
Method	GET
Parameter	
Attack	

Evidence	Age: 597321
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/jquery/ui/core.min.js?ver=1.13.3
Method	GET
Parameter	
Attack	
Evidence	Age: 455154
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/underscore.min.js?ver=1.13.7
Method	GET
Parameter	
Attack	
Evidence	Age: 420004
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/wp-util.min.js?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	Age: 423557
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://virtuestech.com/wp-includes/js/zxcvbn-async.min.js?ver=1.0
Method	GET
Parameter	
Attack	
Evidence	Age: 193525
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	305

Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	
WASC Id	
Plugin Id	10050

INFORMATIONAL	SESSION MANAGEMENT RESPONSE IDENTIFIED
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	https://virtuestech.com/wp-login.php
Method	GET
Parameter	wordpress_test_cookie
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET
Parameter	wordpress_test_cookie
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie

URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	wordpress_test_cookie
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	wordpress_test_cookie
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	wordpress_test_cookie
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	wordpress_test_cookie
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
Instances	6
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://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	liquid-footer
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-footer=footer appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-footer=footer The user-controlled value was: footer
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	liquid-footer
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-footer=footer appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-footer=footer The user-controlled value was: footer - virtue software technologies (virtuestech)
URL	https://virtuestech.com/?liquid-footer=footer
Method	GET
Parameter	liquid-footer
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-footer=footer appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-footer=footer The user-controlled value was: https://virtuestech.com/?liquid-footer=footer
URL	https://virtuestech.com/?liquid-footer=vst-main-footer

Method	GET
Parameter	liquid-footer
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-footer=vst-main-footer appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-footer=vst-main-footer The user-controlled value was: https://virtuestech.com/?liquid-footer=vst-main-footer
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	liquid-header
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-header=header appears to include user input in: a(n) [header] tag [class] attribute The user input found was: liquid-header=header The user-controlled value was: header site-header main-header is-not-stuck
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	liquid-header
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-header=header appears to include user input in: a(n) [header] tag [id] attribute The user input found was: liquid-header=header The user-controlled value was: header
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	liquid-header
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-header=header appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-header=header The user-controlled value was: header
URL	https://virtuestech.com/?liquid-header=header

Method	GET
Parameter	liquid-header
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-header=header appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-header=header The user-controlled value was: header - virtue software technologies (virtuestech)
URL	https://virtuestech.com/?liquid-header=header
Method	GET
Parameter	liquid-header
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-header=header appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-header=header The user-controlled value was: https://virtuestech.com/?liquid-header=header
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	liquid-header
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-header=new-header appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-header=new-header The user-controlled value was: https://virtuestech.com/?liquid-header=new-header
URL	https://virtuestech.com/?liquid-header=new-header
Method	GET
Parameter	liquid-header
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-header=new-header appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-header=new-header The user-controlled value was: new-header
URL	https://virtuestech.com/?liquid-header=new-header

Method	GET
Parameter	liquid-header
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-header=new-header appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-header=new-header The user-controlled value was: new-header - virtue software technologies (virtuestech)
URL	https://virtuestech.com/?liquid-header=vst-main-header
Method	GET
Parameter	liquid-header
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-header=vst-main-header appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-header=vst-main-header The user-controlled value was: https://virtuestech.com/?liquid-header=vst-main-header
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=cs-menu appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=cs-menu The user-controlled value was: cs-menu
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=cs-menu appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=cs-menu The user-controlled value was: cs-menu - virtue software technologies (virtuestech)
URL	https://virtuestech.com/?liquid-mega-menu=cs-menu

Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=cs-menu appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=cs-menu The user-controlled value was: https://virtuestech.com/?liquid-mega-menu=cs-menu
URL	https://virtuestech.com/?liquid-mega-menu=elementor-1025
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=elementor-1025 appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=elementor-1025 The user-controlled value was: https://virtuestech.com/?liquid-mega-menu=elementor-1025
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=is-menu appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=is-menu The user-controlled value was: https://virtuestech.com/?liquid-mega-menu=is-menu
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=is-menu appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=is-menu The user-controlled value was: is-menu
URL	https://virtuestech.com/?liquid-mega-menu=is-menu

Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=is-menu appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=is-menu The user-controlled value was: is-menu - virtue software technologies (virtuestech)
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=menu-cybersecurity The user-controlled value was: https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=menu-cybersecurity The user-controlled value was: menu-cybersecurity
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=menu-cybersecurity The user-controlled value was: menu-cybersecurity - virtue software technologies (virtuestech)
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu

Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=qe-menu appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=qe-menu The user-controlled value was: https://virtuestech.com/?liquid-mega-menu=qe-menu
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=qe-menu appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=qe-menu The user-controlled value was: qe-menu
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=qe-menu appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=qe-menu The user-controlled value was: qe-menu - virtue software technologies (virtuestech)
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=service-offerings appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=service-offerings The user-controlled value was: https://virtuestech.com/?liquid-mega-menu=service-offerings

URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=service-offerings appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=service-offerings The user-controlled value was: service-offerings
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=service-offerings appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=service-offerings The user-controlled value was: service-offerings - virtue software technologies (virtuestech)
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=services appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=services The user-controlled value was: https://virtuestech.com/?liquid-mega-menu=services
URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=services appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=services The user-controlled value was: services

URL	https://virtuestech.com/?liquid-mega-menu=services
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=services appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=services The user-controlled value was: services - virtue software technologies (virtuestech)
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=taas-menu appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=taas-menu The user-controlled value was: https://virtuestech.com/?liquid-mega-menu=taas-menu
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=taas-menu appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=taas-menu The user-controlled value was: taas-menu
URL	https://virtuestech.com/?liquid-mega-menu=taas-menu
Method	GET
Parameter	liquid-mega-menu
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/?liquid-mega-menu=taas-menu appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: liquid-mega-menu=taas-menu The user-controlled value was: taas-menu - virtue software technologies (virtuestech)

URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET
Parameter	action
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php?action=lostpassword appears to include user input in: a(n) [form] tag [id] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	GET
Parameter	action
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/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://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	redirect_to
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	redirect_to
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/wp-admin/
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	redirect_to
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/wp-admin/css/forms.min.css?ver=6.7.2
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	redirect_to
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/wp-admin/css/l10n.min.css?ver=6.7.2
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	redirect_to
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/wp-admin/css/login.min.css?ver=6.7.2
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F

Method	GET
Parameter	redirect_to
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/wp-admin/js/password-strength-meter.min.js?ver=6.7.2
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F
Method	GET
Parameter	redirect_to
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/wp-admin/js/user-profile.min.js?ver=6.7.2
URL	https://virtuestech.com/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/

Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22906 The user-controlled value was: 22906
URL	https://virtuestech.com/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22906 The user-controlled value was: 22906
URL	https://virtuestech.com/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/
Method	POST

Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22906-o1 The user-controlled value was: wpcf7-f15142-p22906-o1
URL	https://virtuestech.com/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22906-o1 The user-controlled value was: wpcf7-f15142-p22906-o1
URL	https://virtuestech.com/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22906-o1 The user-controlled value was: wpcf7-f15142-p22906-o1-ve-textarea-601
URL	https://virtuestech.com/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22906-o1 The user-controlled value was: wpcf7-f15142-p22906-o1-ve-textarea-601
URL	https://virtuestech.com/
Method	POST

Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/
Method	POST
Parameter	text-438
Attack	

Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=20009 The user-controlled value was: 20009
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=20009 The user-controlled value was: 20009
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20009-o1 The user-controlled value was: wpcf7-f15142-p20009-o1
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20009-o1 The user-controlled value was: wpcf7-f15142-p20009-o1
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20009-o1 The user-controlled value was: wpcf7-f15142-p20009-o1-ve-textarea-601
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20009-o1 The user-controlled value was: wpcf7-f15142-p20009-o1-ve-textarea-601
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	email-873
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/ai-driven-test-automation-2/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/ai-driven-test-automation-2/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=21974 The user-controlled value was: 21974
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=21974 The user-controlled value was: 21974
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p21974-o1 The user-controlled value was: wpcf7-f15142-p21974-o1
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p21974-o1 The user-controlled value was: wpcf7-f15142-p21974-o1
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p21974-o1 The user-controlled value was: wpcf7-f15142-p21974-o1-ve-textarea-601
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p21974-o1 The user-controlled value was: wpcf7-f15142-p21974-o1-ve-textarea-601
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	tel-969
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/atlas/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/atlas/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/contact/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/contact/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/contact/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=256 The user-controlled value was: 256
URL	https://virtuestech.com/contact/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=256 The user-controlled value was: 256
URL	https://virtuestech.com/contact/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/contact/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/contact/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p256-o1 The user-controlled value was: wpcf7-f15142-p256-o1
URL	https://virtuestech.com/contact/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p256-o1 The user-controlled value was: wpcf7-f15142-p256-o1
URL	https://virtuestech.com/contact/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p256-o1 The user-controlled value was: wpcf7-f15142-p256-o1-ve-textarea-601
URL	https://virtuestech.com/contact/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p256-o1 The user-controlled value was: wpcf7-f15142-p256-o1-ve-textarea-601
URL	https://virtuestech.com/contact/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/contact/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/contact/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/contact/
Method	POST
Parameter	text-192
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/contact/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/contact/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22566 The user-controlled value was: 22566
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22566 The user-controlled value was: 22566
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22566-o1 The user-controlled value was: wpcf7-f15142-p22566-o1
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22566-o1 The user-controlled value was: wpcf7-f15142-p22566-o1
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22566-o1 The user-controlled value was: wpcf7-f15142-p22566-o1-ve-textarea-601
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22566-o1 The user-controlled value was: wpcf7-f15142-p22566-o1-ve-textarea-601
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/accessibility-usability-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=19466 The user-controlled value was: 19466
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=19466 The user-controlled value was: 19466
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p19466-o1 The user-controlled value was: wpcf7-f15142-p19466-o1
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p19466-o1 The user-controlled value was: wpcf7-f15142-p19466-o1
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p19466-o1 The user-controlled value was: wpcf7-f15142-p19466-o1-ve-textarea-601
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p19466-o1 The user-controlled value was: wpcf7-f15142-p19466-o1-ve-textarea-601
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	email-873
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/advisory-and-transformation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22591 The user-controlled value was: 22591
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22591 The user-controlled value was: 22591
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22591-o1 The user-controlled value was: wpcf7-f15142-p22591-o1
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22591-o1 The user-controlled value was: wpcf7-f15142-p22591-o1
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22591-o1 The user-controlled value was: wpcf7-f15142-p22591-o1-ve-textarea-601
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22591-o1 The user-controlled value was: wpcf7-f15142-p22591-o1-ve-textarea-601
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/agile-and-devops-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=19359 The user-controlled value was: 19359
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=19359 The user-controlled value was: 19359
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p19359-o1 The user-controlled value was: wpcf7-f15142-p19359-o1
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p19359-o1 The user-controlled value was: wpcf7-f15142-p19359-o1
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p19359-o1 The user-controlled value was: wpcf7-f15142-p19359-o1-ve-textarea-601
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p19359-o1 The user-controlled value was: wpcf7-f15142-p19359-o1-ve-textarea-601
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	text-192
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/ai-driven-test-automation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=20738 The user-controlled value was: 20738
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=20738 The user-controlled value was: 20738
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20738-o1 The user-controlled value was: wpcf7-f15142-p20738-o1
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20738-o1 The user-controlled value was: wpcf7-f15142-p20738-o1
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20738-o1 The user-controlled value was: wpcf7-f15142-p20738-o1-ve-textarea-601
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20738-o1 The user-controlled value was: wpcf7-f15142-p20738-o1-ve-textarea-601
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=14382 The user-controlled value was: 14382
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=14382 The user-controlled value was: 14382
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p14382-o1 The user-controlled value was: wpcf7-f15142-p14382-o1
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p14382-o1 The user-controlled value was: wpcf7-f15142-p14382-o1
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p14382-o1 The user-controlled value was: wpcf7-f15142-p14382-o1-ve-textarea-601
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p14382-o1 The user-controlled value was: wpcf7-f15142-p14382-o1-ve-textarea-601
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	email-873
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/api-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=20587 The user-controlled value was: 20587
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=20587 The user-controlled value was: 20587
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20587-o1 The user-controlled value was: wpcf7-f15142-p20587-o1
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20587-o1 The user-controlled value was: wpcf7-f15142-p20587-o1
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20587-o1 The user-controlled value was: wpcf7-f15142-p20587-o1-ve-textarea-601
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20587-o1 The user-controlled value was: wpcf7-f15142-p20587-o1-ve-textarea-601
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	tel-969
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/business-experience-validation/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/business-experience-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22576 The user-controlled value was: 22576
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22576 The user-controlled value was: 22576
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22576-o1 The user-controlled value was: wpcf7-f15142-p22576-o1
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22576-o1 The user-controlled value was: wpcf7-f15142-p22576-o1
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22576-o1 The user-controlled value was: wpcf7-f15142-p22576-o1-ve-textarea-601
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22576-o1 The user-controlled value was: wpcf7-f15142-p22576-o1-ve-textarea-601
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-native-application-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=20754 The user-controlled value was: 20754
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=20754 The user-controlled value was: 20754
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20754-o1 The user-controlled value was: wpcf7-f15142-p20754-o1
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20754-o1 The user-controlled value was: wpcf7-f15142-p20754-o1
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20754-o1 The user-controlled value was: wpcf7-f15142-p20754-o1-ve-textarea-601
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20754-o1 The user-controlled value was: wpcf7-f15142-p20754-o1-ve-textarea-601
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cloud-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22685 The user-controlled value was: 22685
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22685 The user-controlled value was: 22685
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22685-o1 The user-controlled value was: wpcf7-f15142-p22685-o1
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22685-o1 The user-controlled value was: wpcf7-f15142-p22685-o1
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22685-o1 The user-controlled value was: wpcf7-f15142-p22685-o1-ve-textarea-601
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22685-o1 The user-controlled value was: wpcf7-f15142-p22685-o1-ve-textarea-601
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	email-873
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/compliance-and-security-audits/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22561 The user-controlled value was: 22561
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22561 The user-controlled value was: 22561
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22561-o1 The user-controlled value was: wpcf7-f15142-p22561-o1
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22561-o1 The user-controlled value was: wpcf7-f15142-p22561-o1
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22561-o1 The user-controlled value was: wpcf7-f15142-p22561-o1-ve-textarea-601
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22561-o1 The user-controlled value was: wpcf7-f15142-p22561-o1-ve-textarea-601
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	tel-969
Attack	

Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/comprehensive-test-automation-framework/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=19537 The user-controlled value was: 19537
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=19537 The user-controlled value was: 19537
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p19537-o1 The user-controlled value was: wpcf7-f15142-p19537-o1
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p19537-o1 The user-controlled value was: wpcf7-f15142-p19537-o1
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p19537-o1 The user-controlled value was: wpcf7-f15142-p19537-o1-ve-textarea-601
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p19537-o1 The user-controlled value was: wpcf7-f15142-p19537-o1-ve-textarea-601
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	text-192
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/continuous-quality-engineering/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22695 The user-controlled value was: 22695
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22695 The user-controlled value was: 22695
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22695-o1 The user-controlled value was: wpcf7-f15142-p22695-o1
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22695-o1 The user-controlled value was: wpcf7-f15142-p22695-o1
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22695-o1 The user-controlled value was: wpcf7-f15142-p22695-o1-ve-textarea-601
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22695-o1 The user-controlled value was: wpcf7-f15142-p22695-o1-ve-textarea-601
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/cyber-resilience-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/cyber-resilience-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22571 The user-controlled value was: 22571
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22571 The user-controlled value was: 22571
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22571-o1 The user-controlled value was: wpcf7-f15142-p22571-o1
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22571-o1 The user-controlled value was: wpcf7-f15142-p22571-o1
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22571-o1 The user-controlled value was: wpcf7-f15142-p22571-o1-ve-textarea-601
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22571-o1 The user-controlled value was: wpcf7-f15142-p22571-o1-ve-textarea-601
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/data-driven-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22680 The user-controlled value was: 22680
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22680 The user-controlled value was: 22680
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22680-o1 The user-controlled value was: wpcf7-f15142-p22680-o1
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22680-o1 The user-controlled value was: wpcf7-f15142-p22680-o1
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22680-o1 The user-controlled value was: wpcf7-f15142-p22680-o1-ve-textarea-601
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22680-o1 The user-controlled value was: wpcf7-f15142-p22680-o1-ve-textarea-601
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	tel-969
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/devsecops-integration/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/devsecops-integration/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22581 The user-controlled value was: 22581
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22581 The user-controlled value was: 22581
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22581-o1 The user-controlled value was: wpcf7-f15142-p22581-o1
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22581-o1 The user-controlled value was: wpcf7-f15142-p22581-o1
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22581-o1 The user-controlled value was: wpcf7-f15142-p22581-o1-ve-textarea-601
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22581-o1 The user-controlled value was: wpcf7-f15142-p22581-o1-ve-textarea-601
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-and-embedded-systems-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22675 The user-controlled value was: 22675
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22675 The user-controlled value was: 22675
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22675-o1 The user-controlled value was: wpcf7-f15142-p22675-o1
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22675-o1 The user-controlled value was: wpcf7-f15142-p22675-o1
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22675-o1 The user-controlled value was: wpcf7-f15142-p22675-o1-ve-textarea-601
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22675-o1 The user-controlled value was: wpcf7-f15142-p22675-o1-ve-textarea-601
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/iot-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=20790 The user-controlled value was: 20790
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=20790 The user-controlled value was: 20790
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20790-o1 The user-controlled value was: wpcf7-f15142-p20790-o1
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20790-o1 The user-controlled value was: wpcf7-f15142-p20790-o1
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20790-o1 The user-controlled value was: wpcf7-f15142-p20790-o1-ve-textarea-601
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20790-o1 The user-controlled value was: wpcf7-f15142-p20790-o1-ve-textarea-601
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	email-873
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/managed-soc-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=13749 The user-controlled value was: 13749
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=13749 The user-controlled value was: 13749
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p13749-o1 The user-controlled value was: wpcf7-f15142-p13749-o1
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p13749-o1 The user-controlled value was: wpcf7-f15142-p13749-o1
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p13749-o1 The user-controlled value was: wpcf7-f15142-p13749-o1-ve-textarea-601
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p13749-o1 The user-controlled value was: wpcf7-f15142-p13749-o1-ve-textarea-601
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	tel-969
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/manual-testing-services/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22700 The user-controlled value was: 22700
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22700 The user-controlled value was: 22700
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22700-o1 The user-controlled value was: wpcf7-f15142-p22700-o1
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22700-o1 The user-controlled value was: wpcf7-f15142-p22700-o1
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22700-o1 The user-controlled value was: wpcf7-f15142-p22700-o1-ve-textarea-601
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22700-o1 The user-controlled value was: wpcf7-f15142-p22700-o1-ve-textarea-601
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/mobile-security-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=20670 The user-controlled value was: 20670
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=20670 The user-controlled value was: 20670
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20670-o1 The user-controlled value was: wpcf7-f15142-p20670-o1
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20670-o1 The user-controlled value was: wpcf7-f15142-p20670-o1
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20670-o1 The user-controlled value was: wpcf7-f15142-p20670-o1-ve-textarea-601
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20670-o1 The user-controlled value was: wpcf7-f15142-p20670-o1-ve-textarea-601
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/penetration-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=14364 The user-controlled value was: 14364
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=14364 The user-controlled value was: 14364
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p14364-o1 The user-controlled value was: wpcf7-f15142-p14364-o1
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p14364-o1 The user-controlled value was: wpcf7-f15142-p14364-o1
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p14364-o1 The user-controlled value was: wpcf7-f15142-p14364-o1-ve-textarea-601
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p14364-o1 The user-controlled value was: wpcf7-f15142-p14364-o1-ve-textarea-601
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	email-873
Attack	

Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/performance-engineering-monitoring/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22690 The user-controlled value was: 22690
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22690 The user-controlled value was: 22690
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22690-o1 The user-controlled value was: wpcf7-f15142-p22690-o1
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22690-o1 The user-controlled value was: wpcf7-f15142-p22690-o1
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22690-o1 The user-controlled value was: wpcf7-f15142-p22690-o1-ve-textarea-601
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22690-o1 The user-controlled value was: wpcf7-f15142-p22690-o1-ve-textarea-601
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	tel-969
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/secure-code-validation/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/secure-code-validation/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22586 The user-controlled value was: 22586
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22586 The user-controlled value was: 22586
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22586-o1 The user-controlled value was: wpcf7-f15142-p22586-o1
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22586-o1 The user-controlled value was: wpcf7-f15142-p22586-o1
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22586-o1 The user-controlled value was: wpcf7-f15142-p22586-o1-ve-textarea-601
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22586-o1 The user-controlled value was: wpcf7-f15142-p22586-o1-ve-textarea-601
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/shift-left-and-shift-right-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/shift-left-and-shift-right-testing/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=20606 The user-controlled value was: 20606
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=20606 The user-controlled value was: 20606
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20606-o1 The user-controlled value was: wpcf7-f15142-p20606-o1
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20606-o1 The user-controlled value was: wpcf7-f15142-p20606-o1
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20606-o1 The user-controlled value was: wpcf7-f15142-p20606-o1-ve-textarea-601
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20606-o1 The user-controlled value was: wpcf7-f15142-p20606-o1-ve-textarea-601
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	text-438
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/test-center-of-excellence/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=20732 The user-controlled value was: 20732
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=20732 The user-controlled value was: 20732
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20732-o1 The user-controlled value was: wpcf7-f15142-p20732-o1
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20732-o1 The user-controlled value was: wpcf7-f15142-p20732-o1
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20732-o1 The user-controlled value was: wpcf7-f15142-p20732-o1-ve-textarea-601
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p20732-o1 The user-controlled value was: wpcf7-f15142-p20732-o1-ve-textarea-601
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	email-873
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/vulnerability-assessment/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [div] tag [data-wpcf7-id] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7=15142 The user-controlled value was: 15142
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: _wpcf7_container_post=22708 The user-controlled value was: 22708
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_container_post=22708 The user-controlled value was: 22708
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7_locale
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: _wpcf7_locale=en_US The user-controlled value was: en_us
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [div] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22708-o1 The user-controlled value was: wpcf7-f15142-p22708-o1
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22708-o1 The user-controlled value was: wpcf7-f15142-p22708-o1
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [li] tag [id] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22708-o1 The user-controlled value was: wpcf7-f15142-p22708-o1-ve-textarea-601
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [textarea] tag [aria-describedby] attribute The user input found was: _wpcf7_unit_tag=wpcf7-f15142-p22708-o1 The user-controlled value was: wpcf7-f15142-p22708-o1-ve-textarea-601
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpcf7_version=6.0.5 The user-controlled value was: 6.0.5
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email-873=foo-bar@example.com The user-controlled value was: foo-bar@example.com
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	tel-969
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: tel-969=9999999999 The user-controlled value was: 9999999999
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-192=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/services/zero-trust-network-assessments/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: text-438=ZAP The user-controlled value was: zap
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	redirect_to
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	redirect_to
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/wp-admin/
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	redirect_to
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/wp-admin/css/forms.min.css?ver=6.7.2
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	redirect_to
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/wp-admin/css/l10n.min.css?ver=6.7.2
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	redirect_to
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/wp-admin/css/login.min.css?ver=6.7.2
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	redirect_to
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/wp-admin/js/password-strength-meter.min.js?ver=6.7.2
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	redirect_to
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=https://virtuestech.com/wp-admin/ The user-controlled value was: https://virtuestech.com/wp-admin/js/user-profile.min.js?ver=6.7.2
URL	https://virtuestech.com/wp-login.php
Method	POST
Parameter	rememberme
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/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://virtuestech.com/wp-login.php
Method	POST
Parameter	wp-submit
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/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://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	action
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/wp-login.php?action=lostpassword appears to include user input in: a(n) [form] tag [id] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	action
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/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://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	user_login
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/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://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	wp-submit
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://virtuestech.com/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	522
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

Sequence Details

With the associated active scan results.