



Vulnerability Scan Report



ZAP Scanning Report

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

Generated on Tue, 15 Apr 2025 15:34:20

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	433
Strict-Transport-Security Header Not Set	Low	724
Timestamp Disclosure - Unix	Low	574
X-Content-Type-Options Header Missing	Low	533
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	102
Session Management Response Identified	Informational	5
User Controllable HTML Element Attribute (Potential XSS)	Informational	522

Alert Detail

Medium	Absence of Anti-CSRF Tokens
--------	---

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a 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:

Description

- * 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">

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	<pre><form action="/#wpcf7-f15142-p22906-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init"></pre>
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	<pre><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"></pre>
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	<pre><form action="/atlas/#wpcf7-f15142-p21974-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init"></pre>
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	<pre><form action="/contact/#wpcf7-f15142-p256-o1" method="post" class="wpcf7-form init" aria-label="Contact form" novalidate="novalidate" data-status="init"></pre>

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">

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">

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">

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">

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-ac

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	<pre><form action="/contact/#wpcf7-f15142-p256-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid"></pre>
Other Info	<p>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"].</p>
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	
Attack	
Evidence	<pre><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"></pre>
Other Info	<p>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"].</p>
URL	https://virtuestech.com/services/advisory-and-transformation/
Method	POST
Parameter	
Attack	
Evidence	<pre><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"></pre>
Other Info	<p>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"].</p>
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	

Attack

```
<form action="/services/agile-and-devops-testing/#wpcf7-f15142-p22591-o1" method="post"
```

Evidence 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

```
<form action="/services/ai-driven-test-automation/#wpcf7-f15142-p19359-o1" method="post"
```

Evidence 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

```
<form action="/services/api-security-testing/#wpcf7-f15142-p20738-o1" method="post"
```

Evidence 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

```
<form action="/services/api-testing-services/#wpcf7-f15142-p14382-o1" method="post"
```

Evidence 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

```
<form action="/services/business-experience-validation/#wpcf7-f15142-p20587-o1"
```

Evidence 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

```
<form action="/services/cloud-native-application-testing/#wpcf7-f15142-p22576-o1"
```

Evidence 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

```
<form action="/services/cloud-security-testing/#wpcf7-f15142-p20754-o1" method="post"
```

Evidence 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

```
<form action="/services/compliance-and-security-audits/#wpcf7-f15142-p22685-o1"
```

Evidence 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

```
<form action="/services/comprehensive-test-automation-framework/#wpcf7-f15142-p22561-o1"
```

Evidence 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

```
<form action="/services/continuous-quality-engineering/#wpcf7-f15142-p19537-o1"
```

Evidence `method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">`

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf,

Other Info `_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

```
<form action="/services/cyber-resilience-testing/#wpcf7-f15142-p22695-o1" method="post"
```

Evidence `class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">`

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf,

Other Info `_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

```
<form action="/services/data-driven-testing/#wpcf7-f15142-p22571-o1" method="post"
```

Evidence `class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">`

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf,

Other Info `_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

```
<form action="/services/devsecops-integration/#wpcf7-f15142-p22680-o1" method="post"
```

Evidence 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

```
<form action="/services/iot-and-embedded-systems-testing/#wpcf7-f15142-p22581-o1"
```

Evidence 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

```
<form action="/services/iot-security-testing/#wpcf7-f15142-p22675-o1" method="post"
```

Evidence 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

```
<form action="/services/managed-soc-services/#wpcf7-f15142-p20790-o1" method="post"
```

Evidence 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

```
<form action="/services/manual-testing-services/#wpcf7-f15142-p13749-o1" method="post"
```

Evidence 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

```
<form action="/services/mobile-security-testing/#wpcf7-f15142-p22700-o1" method="post"
```

Evidence 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

```
<form action="/services/penetration-testing/#wpcf7-f15142-p20670-o1" method="post"
```

Evidence 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-Engineering-Monitoring/>

Method POST

Parameter

Attack

```
<form action="/services/penetration-Engineering-Monitoring/#wpcf7-f15142-p14364-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">
```

Evidence 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"].

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-engineering-monitoring/>

Method POST

Parameter

Attack

```
<form action="/services/penetration-engineering-monitoring/#wpcf7-f15142-p14364-o1" method="post" class="wpcf7-form invalid" aria-label="Contact form" novalidate="novalidate" data-status="invalid">
```

Evidence 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"].

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

```
<form action="/services/secure-code-validation/#wpcf7-f15142-p22690-o1" method="post"
```

Evidence 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

```
<form action="/services/shift-left-and-shift-right-testing/#wpcf7-f15142-p22586-o1"
```

Evidence 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

```
<form action="/services/test-center-of-excellence/#wpcf7-f15142-p20606-o1" method="post"
```

Evidence 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	<pre><form name="lostpasswordform" id="lostpasswordform" action="https://virtuestech.com/wp-login.php?action=lostpassword" method="post"></pre>
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
	<p>Phase: Architecture and Design</p> <p>Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.</p> <p>For example, use anti-CSRF packages such as the OWASP CSRFGuard.</p>
	<p>Phase: Implementation</p> <p>Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.</p>
	<p>Phase: Architecture and Design</p> <p>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).</p>
Solution	<p>Note that this can be bypassed using XSS.</p> <p>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.</p> <p>Note that this can be bypassed using XSS.</p> <p>Use the ESAPI Session Management control.</p> <p>This control includes a component for CSRF.</p> <p>Do not use the GET method for any request that triggers a state change.</p> <p>Phase: Implementation</p> <p>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.</p>

Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.pdf
CWE Id	352
WASC Id	9
Plugin Id	10202
Medium	CSP: Failure to Define Directive with No Fallback
Description	<p>The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding them is the same as allowing anything.</p>
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/
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-ac	
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. 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_res
Reference	
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/
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-ac
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.
	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_res

CWE Id	693
WASC Id	15
Plugin Id	10055
Medium	CSP: script-src unsafe-inline
Description	<p>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.</p>
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	
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-ac
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. 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/
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-ac

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	<p>https://www.w3.org/TR/CSP/</p> <p>https://caniuse.com/#search=content+security+policy</p> <p>https://content-security-policy.com/</p> <p>https://github.com/HtmlUnit/htmlunit-csp</p> <p>https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources</p>
CWE Id	693
WASC Id	15
Plugin Id	10055
Medium	Content Security Policy (CSP) Header Not Set

Description	<p>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.</p>
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	<p>Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.</p> <p>https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy</p>
Reference	<p>https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html</p> <p>https://www.w3.org/TR/CSP/</p> <p>https://w3c.github.io/webappsec-csp/</p> <p>https://web.dev/articles/csp</p> <p>https://caniuse.com/#feat=contentsecuritypolicy</p> <p>https://content-security-policy.com/</p>
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>

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
	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.
Solution	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	The identified library jquery-ui, version 1.13.1 is vulnerable. CVE-2022-31160
Info	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%2Fwp-login.php

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-ac
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="5c1cbd5e90e49d80b9525962-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="a2742f12c9954e648040752c-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	

URL <https://virtuestech.com/>

Method GET

Parameter https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="551335e7b8d8541cdc5a016e-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="48dceae89c568fbc5a3a48cf-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="589002a69365c46811be6261-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="1d4e6e30cdad59d4962fd264-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="5ba68482588908001d7064e1-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="edc44ccbdb62ec3425d63be5-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence	<pre><script type="613a92b85cb061db4684d853-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=is-menu
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="86e352baf5a3c79d779e4320-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=menu-cybersecurity
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="80e4086a0ed9312bddeebecb-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=qe-menu
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="742c52e5ad78203ffa14a6d6-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/?liquid-mega-menu=service-offerings
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="b1c529018783612da17a2c95-text/javascript"

Evidence

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8&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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="7f07322b113e6df15698ee9d-text/javascript"

Evidence

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8&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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="428b9e3e696b9411fc764097-text/javascript"

Evidence

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8&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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="b4ff7bd33a0fee176e23d10b-text/javascript"

Evidence

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8&id=google-recaptcha-js"></script>

Other

Info

URL

<https://virtuestech.com/about/>

Method

GET

Parameter <https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="e5e4af171f4f1922902dbe93-text/javascript"

Evidence [src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8"](https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8)
id="google-recaptcha-js"></script>

Other
Info

URL <https://virtuestech.com/advisorytransformation>

Method GET

Parameter <https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="97f3c2df894f7e692f82206a-text/javascript"

Evidence [src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8"](https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8)
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="ae65deffef5c55a3f174da75-text/javascript"

Evidence [src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8"](https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8)
id="google-recaptcha-js"></script>

Other
Info

URL <https://virtuestech.com/atlas/>

Method GET

Parameter <https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="0992651c94b560aeaeaf89ff-text/javascript"

Evidence [src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8"](https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8)
id="google-recaptcha-js"></script>

Other
Info

URL <https://virtuestech.com/author/virtuestech/>

Method GET

Parameter <https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="0a6ef5d45184e6bb8d7d9759-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="1f97883ce7750b0215b0cdeb-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" id="google-recaptcha-js"></script>

Other Info

URL <https://virtuestech.com/blogs/>

Method GET

Parameter <https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="f8d31655ba0fe65fd1719fd7-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" id="google-recaptcha-js"></script>

Other Info

URL <https://virtuestech.com/careers/>

Method GET

Parameter <https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="097e1e315dbf0374dcf48719-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="d5baec9fdcd9a614f8142a64-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="07054652c019fa2c02675d4f-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="7628343e668ad4107c03dd75-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="9477513ac96c722cb5e4011c-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
id="google-recaptcha-js"></script>

Other
Info

URL <https://virtuestech.com/category/uncategorized/>

Method GET

Parameter https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="246c6acdd6a805fec4e30982-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
id="google-recaptcha-js"></script>

Other
Info

URL <https://virtuestech.com/contact/>

Method GET

Parameter https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="ab67da4099f231817f540d3a-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
id="google-recaptcha-js"></script>

Other
Info

URL <https://virtuestech.com/cybersecurity-services/>

Method GET

Parameter https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="b9adaa7e65cc342a4d049a6a-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence	<pre><script type="eefc1a56c90322b4b4e02b9c-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/importance-of-performance-testing-and-monitoring/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="4f4c16cf22dc849b38becaa3-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/industries/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="b84eb814df2fdf5e2e118508-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/insights/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="117a8cc0b8a962035624166c-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/services/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="153431c2bc644cd36377baff-text/javascript"

Evidence

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="7afd31d67b1bfcd22906a640-text/javascript"

Evidence

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="529cdb58f519920351e2319d-text/javascript"

Evidence

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="9028185f5c3dc221ba869609-text/javascript"

Evidence

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

Evidence <script type="0bd7a8cfec6f5e1259276b-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

Evidence <script type="3a03eaf674bb59457440550d-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

Evidence <script type="762b3138e26b4d53fb317083-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

Evidence <script type="3f9ade541151e87472a24a9e-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

```
<script type="ddf44dd24895d926380ecc63-text/javascript"
```

Evidence `src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8"`
`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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

```
<script type="af52bcd2a42b26f55161113e-text/javascript"
```

Evidence `src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8"`
`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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

```
<script type="ec0bc461ed7f072c564f8afd-text/javascript"
```

Evidence `src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8"`
`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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

```
<script type="d2bfe161797371a8e69d3c04-text/javascript"
```

Evidence `src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8"`
`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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="c20df706a356922e0d5ba18c-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="fa58adaa7fb9ef1ebd5f0cc5-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="1e1444ad55d8adf006edd7b7-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="f43c45761617bc3b5ddafbb7-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="fb9ac87beed01e209d24c378-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="0d2873224088439b3c3c2b86-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="44257a1d4df7443c30ad2191-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence	<pre><script type="5f12bed1908b6f981b108c45-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/services/mobile-security-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="2b043f5df93330a2cf6a36e5-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/services/penetration-testing/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="44eb2d279437b1438e5e3800-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/services/performance-Engineering-Monitoring/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="b6c42c28aa216518ba71937d-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/services/performance-engineering-monitoring/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="fe39e337acc7234ede1c5ddb-text/javascript"

Evidence

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="dd004bf67f0034b5cba6f569-text/javascript"

Evidence

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="802690703af08a97f53adf69-text/javascript"

Evidence

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

<script type="9ee1120fd6b2c24689087b6b-text/javascript"

Evidence

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="f9820c935faa1d4cb3e03c9f-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="e4d5dbc97cc6666037720055-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="da03cb834ada913a5bd49145-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="4e8da7e05ede99794ff67847-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="12762e4942fac1c0dd6cc6fa-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="f0f9e9a8cfec73123473531f-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="6a8bfaa44042ed64983c6ed6-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="99c932585309b80bd0e20eca-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="5205696bfa0800fcaadf6f15-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="5e0ddfa4ccdae7d1a9fc36eb-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="bfd57d2e88bb3d1405919836-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="312efa379235b0394c111cb9-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="0d3e6c8c461706b81d178ae8-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="cbb33e2f4618f0f51df7971a-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="99f6675e055afef7f0a62dd8-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence	<pre><script type="ac7a54dfd1c9e74eaf62aa2b-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="e2c42bada349e771a8eb0c6b-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="b7e16ff4b44c445874cf233b-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="099333b929f8a90631fe7612-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="9e6b60b04d83fd9d3037fabb-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="google-recaptcha-js"></script>

Other

Info

URL <https://virtuestech.com/>

Method POST

Parameter https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="fad4593dc6edd438f516ea78-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="1c0eeba5b7b19887f17bb7bf-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="google-recaptcha-js"></script>

Other

Info

URL <https://virtuestech.com/atlas/>

Method POST

Parameter https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="d5a6410d74c751c28b7a6d4b-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="google-recaptcha-js"></script>

Other

Info

URL <https://virtuestech.com/contact/>

Method POST

Parameter <https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="719788da5619b367c107ffca-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="bd28bc4fea02b04dcfd25daf-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="6fc69aff0e8eb675567f9847-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="793eea776d624f6cd9ead103-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

```
<script type="a78c5c21b83b41d8d639fb9e-text/javascript"
```

Evidence `src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8"`
`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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

```
<script type="1d9e8b38def102174b3405c1-text/javascript"
```

Evidence `src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8"`
`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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

```
<script type="c2e739f9beec040b41ef233-text/javascript"
```

Evidence `src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8"`
`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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

```
<script type="e9231bd8fc8f4fb772154449-text/javascript"
```

Evidence `src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8"`
`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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="07e73417d80ac14ec9ac10bc-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="f3e666081d0dd0f97213df9c-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="2b1e61b352051b0662457724-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="a77433499cbeed33bf1bcfad-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="7f92e352896033b075e23b79-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="b5cbd396e5dddf243d8c4bf0-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence <script type="e995fa0788fb860ae013ca19-text/javascript"
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNc
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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

Evidence	<pre><script type="1af858a39a8e7e85438f39bd-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="f739700657b153ba1f23f156-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="9951db35c4b4cd2cc0f91a85-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8
Attack	
Evidence	<pre><script type="0a4f0db8912d6efc727a99c8-text/javascript" src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8 id="google-recaptcha-js"></script></pre>
Other Info	
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

```
<script type="3a9e0bab36fa9fce28bee845-text/javascript"
```

Evidence

```
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

```
<script type="18dffcc2c77170a34bc0fefd-text/javascript"
```

Evidence

```
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="google-recaptcha-js"></script>
```

Other

Info

URL

<https://virtuestech.com/services/penetration-testing/>

Method POST

Parameter https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

```
<script type="54ce621ddf357a2ee443d3bb-text/javascript"
```

Evidence

```
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8

Attack

```
<script type="5619f7c9da04569de7a5778a-text/javascript"
```

Evidence

```
src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8id="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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

Evidence <script type="c3b9a0927df38b91e37f5078-text/javascript"

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

Evidence <script type="110088178e6927b83ae0f9ef-text/javascript"

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

Evidence <script type="cdd1d5506ff266c49c825c2d-text/javascript"

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

Evidence <script type="0f0eedb51ef6cc4837b68f31-text/javascript"

src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="45f8b6bc0e354659a0bb3e34-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8>

Attack

<script type="ede249707625f95954a4f328-text/javascript"

Evidence src="https://www.google.com/recaptcha/api.js?render=6LdGkQwrAAAAAJUFwQdGCYH9giwaPdqFINNcCZLi8" 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/advisory/transformation>

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/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	
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

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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-1%2Fpost-1%2F>

Method GET

Parameter

Attack

Evidence X-Powered-By: PHP/8.2.27

Other
Info

Method GET

Parameter

Attack

Evidence X Powered By: PPTW 8.2.27

Info

URL <https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence X-Powered-By: PHP/8.2.27

Other Info

URL

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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence X-Powered-By: PHP/8.2.27

Other Info

URL

Method GET

Parameter

Attack

Evidence X-Powered-By: PHP/8.2.27

Other Info

URL

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%2Findex.html>

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%2Findex.html>

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%2Findex.html>

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%2Findex.html>

Method GET

Parameter

Attack

Evidence X-Powered-By: PHP/8.2.27

Other
Info

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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-1%2Fpost-1%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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence X-Powered-By: PHP/8.2.27

Other
Info

URI: <https://virtuotech.com/vn.json?embed/1.0/embed2format.xml&url=https%3A%2F%2Fvirtuotech.com%2Fvirtuotech.com-vn.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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-1%2Fpost-1%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%2Fcategory%2Fcategory-1%2Fpost-1%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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Findex.html>

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%2Findex.html>

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%2Findex.html>

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%2Findex.html>

Method GET

Parameter

Attack

Evidence X-Powered-By: PHP/8.2.27

Other
Info

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%2Fvirtuestech.com>

Method GET

Parameter

Attack

Evidence X-Powered-By: PHP/8.2.27

Other Info

URL

Method GET

Parameter

Attack

Evidence X-Powered-By: PHP/8.2.27

Other Info

URL

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

URI: <https://virtuotech.com/vn.json?embed/1.0/embed2format.xml&url=https%3A%2F%2Fvirtuotech.com%2Fvirtuotech.com-vn.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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-1%2Fpost-1%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&uri=https%3A%2F%2Fvirtuestech.com%2Fcategory%2Fcategory-1%2Fpost-1%2F>

Method GET

Parameter

Attack

Evidence X Powered By: PPTW 8.2.27

Info

URL <https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Findex.html>

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%2Findex.html>

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%2Findex.html>

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%2Findex.html>

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%2Fliquido
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%2Fliquido
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%2Fliquido
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%2Fliquido
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%2Fliquido
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%3Fliquic>

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%3Fliquic>

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%3Fliquic>

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%3Fliquic>

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%3D1
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%3D1
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%3D1
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%3D1
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%3D1

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%3Fliquic>

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%3Fliquic>

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->

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-prac>

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%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%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%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%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%2Findex.html
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%2Findex.html
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%2Findex.html
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%2Findex.html
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%2Findex.html

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%2Fcategory%2Fphp%2Findex.php>

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%2Fcategory%2Fphp%2Findex.php>

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%2Fcategory%2Fphp%2Findex.php>

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%2Fcategory%2Fphp%2Findex.php>

Method GET

Parameter

Attack

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%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%2F>

Method GET

Parameter

Attack

Evidence X-Powered-By: PHP/8.2.27

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>

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-th>

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-in>

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-ac

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/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	433
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-Introduction_to_Web_Security/Test_Environment/01-Header_Review 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/>

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=6.0.6>

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/plugins/contact-form-7/includes/js/index.js?ver=6.0.6>

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/plugins/contact-form-7/includes/swv/js/index.js?ver=6.0.6>

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/plugins/contact-form-7/modules/recaptcha/index.js?ver=6.0.6>

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/fontawesome/js/v4-shims.min.js?ver=3.2.1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/hub-core/extras/redux-framework/redux-core/assets/css/extended.css?ver=5.0.1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/hub-elementor-addons/assets/css/blog/blog-single/blog-single.css?ver=5.0.1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/hub-elementor-addons/assets/css/pages/not-found.css?ver=5.0.1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/plugins/hub-elementor-addons/assets/css/theme-elementor.min.css?ver=5.0.1
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-essenti>

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/themes/hub/assets/vendors/liquid-icon/lqd-essentials/lqd-essentials.mi>

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/themes/hub/assets/vendors/liquid-icon/lqd-essentials/lqd-essentials.mi>

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.jpg>

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-e1730117154990-1024>

Method GET

Parameter

Attack

Evidence

Other
Info

URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-1536x300.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-2048x300.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-300x300.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/10/Cloud-Security-Testing-Blog-e1730117154990-768x300.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-e17297>

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-e17297>

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-e17297>

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-e172>

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-1>

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-2>

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-3>

Method GET

Parameter

Attack

Evidence

Other
Info

URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-0
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring-1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/2024/11/Importance-of-Performance-Testing-and-Monitoring.j
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.jpeg

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/uploads/2025/04/Underline03.png>

Method GET

Parameter

Attack

Evidence

Other
Info

URL	https://virtuestech.com/wp-content/uploads/elementor/css/custom-apple-webkit.min.css?ver=1744710319
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/css/custom-frontend.min.css?ver=1744710319
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/css/aleo.css?ver=1744452449
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=17440>

Method GET

Parameter

Attack

Evidence

Other

Info

URL https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/aleo-c4mh1nf8g8_swaj50xvs.w

Method GET

Parameter

Attack

Evidence

Other

Info

URL

https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/aleo-c4mh1nf8g8_swaj53bvsooy

Method GET

Parameter

Attack

Evidence

Other

Info

URL

https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/aleo-c4mh1nf8g8_swaj53rvsooy

Method GET

Parameter

Attack

Evidence

Other

Info

URL

https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/aleo-c4mv1nf8g8_swa3j0q.woff2

Method GET

Parameter

Attack

Evidence

Other

Info

URL

https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/aleo-c4mv1nf8g8_swaj0q1o.woff2

Method GET

Parameter

Attack

Evidence

Other

Info

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/aleo-c4mv1nf8q8_swapj0q1o.w
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqq7ca725
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqq7ca725
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqq7ca725
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqq7ca725
Method	GET
Parameter	

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqq7ca725>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqq7ca725>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc53fwrk3iltcvneqq7ca725>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmx

Method GET

Parameter

Attack

Evidence

Other
Info

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmx
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmx
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmx
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmx
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrmx

Method GET

Parameter

Attack

Evidence

Other

Info

URL

https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/inter-ucc73fwrk3iltehus_nvmrrmx

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba>

Method GET

Parameter

Attack

Evidence

Other

Info

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memtyags126mizpba
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba
Method	GET
Parameter	

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba>

Method GET

Parameter

Attack

Evidence

Other
Info

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/opensans-memvyags126mizpba
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxiayp8kv8jhgfvrljlme0t

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxiayp8kv8jhgfvrlme0tr>

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlbt5z1j>

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlbt5z1x>

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlcz7z1>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvr1cz7z1x>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvr1dd4z1>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvr1dd4z1>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrldz8z1>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrldz8z1x1>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrljej6z1j1>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrljej6z1x1>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlfj_z1j1f

Method GET

Parameter

Attack

Evidence

Other
Info

URL

https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlfj_z1x1

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlgt9z1j>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxibyp8kv8jhgfvrlgt9z1x>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrljm111>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrljm111>

Method GET

Parameter

Attack

Evidence

Other
Info

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrijlm21x
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrijlm21x
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrijlm81x
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrijlm81x
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrijlm91x

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrijlmg1h>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrijlmr19>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrijlmr19>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrijlmv1p>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrljlmv1p>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrljlmv15>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxidyp8kv8jhgfvrljlmv15>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxieyp8kv8jhgfvrljfecg>

Method GET

Parameter

Attack

Evidence

Other

Info

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxieyp8kv8jhgfvrijnecm
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrijluchta
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrijlufnta
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrlptuchta
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/poppins-pxigyp8kv8jhgfvrlptufnta
Method	GET
Parameter	

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec>

Method GET

Parameter

Attack

Evidence

Other
Info

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo5cnqeu92fr1mu53zec

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter

Attack

Evidence

Other

Info

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/roboto-kfo7cnqeu92fr1me7ksn6
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5
Method	GET
Parameter	

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5>

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5>

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5>

Method GET

Parameter

Attack

Evidence

Other
Info

URL <https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievj2zhzi2ecn5>

Method GET

Parameter

Attack

Evidence

Other
Info

URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-iev12zhzi2ecn5
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-iev12zhzi2ecn5
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-iev12zhzi2ecn5
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-iev12zhzi2ecn5
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-iev12zhzi2ecn5

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-content/uploads/elementor/google-fonts/fonts/robotocondensed-ievl2zhzi2ecn5>

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%2Fvirtuestech.com>

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%2Fvirtuestech.com>

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%2Fvirtuestech.com>

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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

Other Info

URL

Method GET

Parameter

Attack

Evidence

Other Info

URL

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

Attack

Evidence

Other Info

URL

<https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

Other

URL

Method GET

Parameter

Attack

Evidence

Other Info

URL

Method GET

Parameter

Attack

Evidence

Other Info

URL

Method GET

Parameter

Attack

Evidence

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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

Other Info

URL

Method GET

Parameter

Attack

Evidence

Other Info

URL

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

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

Other

URL

Method GET

Parameter

Attack

Evidence

Other Info

URL

Method GET

Parameter

Attack

Evidence

Other Info

URL

Method GET

Parameter

Attack

Evidence

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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

Other Info

URL

Method GET

Parameter

Attack

Evidence

Other Info

URL

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

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
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
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%3Fliquic>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquic>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquic>

Method GET

Parameter

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquic>

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
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
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
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
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

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquic>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquic>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquic>

Method GET

Parameter

Attack

Evidence

Other

Info

URL

<https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2F%3Fliquic>

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%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-prac%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%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%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%2Fcategory%2Fmobile%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%2Fcategory%2Fmobile%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%2Fcategory%2Fmobile%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%2Fcategory%2Fmobile%2F>

Method GET

Parameter

Attack

Evidence

Method GET

Parameter

Attack

Evidence

Other

Info

URL <https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcategory%2Fcategory-name%2Fpost%2Fpost-name>

Method GET

Parameter

Attack

Evidence

Other

Info

URL <https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcategory%2Fcategory-name%2Fpost%2Fpost-name>

Method GET

Parameter

Attack

Evidence

Other

Info

URL <https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcategory%2Fcategory-name%2Fpost%2Fpost-name>

Method GET

Parameter

Attack

Evidence

Other

Info

URL <https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fservices%2Fcategory%2Fcategory-name%2Fpost%2Fpost-name>

Method GET

Parameter

Attack

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

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%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

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-e>

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-in>

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>

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-th>

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-in>

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-ac

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	724
Solution	<p>Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.</p> <p>https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html</p>
Reference	<p>https://owasp.org/www-community/Security_Headers</p> <p>https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security</p> <p>https://caniuse.com/stricttransportsecurity</p> <p>https://datatracker.ietf.org/doc/html/rfc6797</p>
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 1744452449

Other Info 1744452449, which evaluates to: 2025-04-12 15:37:29.

URL <https://virtuestech.com>

Method GET

Parameter

Attack

Evidence 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744452449	
Other Info	1744452449, which evaluates to: 2025-04-12 15:37:29.	
URL	https://virtuestech.com/	
Method	GET	
Parameter		
Attack		
Evidence	1744710319	
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.	
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

URL <https://virtuestech.com/ai-driven-test-automation-2/embed/>

Method GET

Parameter

Attack

Evidence 1473893002

Other Info 1473893002, which evaluates to: 2016-09-15 04:13:22.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

URL <https://virtuestech.com/atlas/embed/>

Method GET

Parameter

Attack

Evidence 1709820854

Other Info 1709820854, which evaluates to: 2024-03-07 19:44:14.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319	
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.	
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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	1744710319	
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.	
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

URL <https://virtuestech.com/importance-of-performance-testing-and-monitoring/embed/>

Method GET

Parameter

Attack

Evidence 1997237719

Other Info 1997237719, which evaluates to: 2033-04-16 09:45:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

URL <https://virtuestech.com/services/cloud-security-testing/embed/>

Method GET

Parameter

Attack

Evidence 1833117231

Other Info 1833117231, which evaluates to: 2028-02-02 20:43:51.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

URL <https://virtuestech.com/services/manual-testing-services/embed/>

Method GET

Parameter

Attack

Evidence 1444357870

Other Info	1444357870, which evaluates to: 2015-10-09 08:01:10.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

URL <https://virtuestech.com/services/penetration-testing/embed/>

Method GET

Parameter

Attack

Evidence 1691433348

Other Info 1691433348, which evaluates to: 2023-08-08 00:05:48.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

URL <https://virtuestech.com/services/test-center-of-excellence/embed/>

Method GET

Parameter

Attack

Evidence 2047989296

Other Info 2047989296, which evaluates to: 2034-11-24 19:24:56.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319	
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.	
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

URL <https://virtuestech.com/why-cloud-security-testing-is-essential/embed/>

Method GET

Parameter

Attack

Evidence 1660947288

Other Info 1660947288, which evaluates to: 2022-08-20 03:44:48.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744452449

Other Info 1744452449, which evaluates to: 2025-04-12 15:37:29.

URL <https://virtuestech.com/>

Method POST

Parameter

Attack

Evidence 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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 1744710319

Other Info 1744710319, which evaluates to: 2025-04-15 15:15:19.

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	1744710319
Other Info	1744710319, which evaluates to: 2025-04-15 15:15:19.
Instances	574

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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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=6.0.6>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL <https://virtuestech.com/wp-content/plugins/contact-form-7/includes/js/index.js?ver=6.0.6>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL <https://virtuestech.com/wp-content/plugins/contact-form-7/includes/swv/js/index.js?ver=6.0.6>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL <https://virtuestech.com/wp-content/plugins/contact-form-7/modules/recaptcha/index.js?ver=6.0.6>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL <https://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=3.2.1>

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-content/plugins/elementor/assets/lib/font-awesome/js/v4-shims.min.js?ver=3.2.1>

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-content/plugins/hub-core/extras/redux-framework/redux-core/assets/css/extended-rtl.css?ver=3.2.1>

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-content/plugins/hub-elementor-addons/assets/css/blog/blog-single/blog-single.css?ver=3.2.1>

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-content/plugins/hub-elementor-addons/assets/css/pages/not-found.css?ver=5.1.1>

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-content/plugins/hub-elementor-addons/assets/css/theme-elementor.min.css?ver=5.1.1>

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-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-essenti>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their 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.mi>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their 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.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/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.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.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

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-e1730117154990-1024x300x>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-e1730117154990-1536x300x>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-e1730117154990-2048x300x>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-e1730117154990-300x300x>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-e1730117154990-768x320.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-e17297>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-e17297>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-e172976>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-e172>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-1.pdf>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-2.pdf>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-3.pdf>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-4.pdf>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-1.pdf>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-1.pdf>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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/kagooollogo.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.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/Underline03.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/elementor/css/custom-apple-webkit.min.css?ver=1744710319>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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=1744710319>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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/aleo.css?ver=1744452449>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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=174409>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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/aleo-c4mh1nf8q8_swaj50xvs.w

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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/aleo-c4mh1nf8q8_swaj53bvsooy

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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/aleo-c4mh1nf8q8_swaj53rvsooy

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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/aleo-c4mv1nf8g8_swa3j0q.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/aleo-c4mv1nf8g8_swaj0q1o.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/aleo-c4mv1nf8g8_swapj0q1o.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-ucc53fwrk3iltcvneqq7ca725.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-ucc53fwrk3iltcvneqq7ca725>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ucc53fwrk3iltcvneqq7ca725>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ucc53fwrk3iltcvneqq7ca725>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ucc53fwrk3iltcvneqq7ca725>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ucc53fwrk3iltcvneqq7ca725>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ucc53fwrk3iltcvneqq7ca725>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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_nvmrmx

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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_nvmrmx

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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_nvmrmx

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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_nvmrmx

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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_nvmrmx

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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_nvmrrmx

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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_nvmrrmx

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxiayp8kv8jhgfvrjlme0t>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxiayp8kv8jhgfvrjlme0tr>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxibyp8kv8jhgfvrllbt5z1j>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxibyp8kv8jhgfvrllbt5z1x>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxibyp8kv8jhgfvrllcz7z1>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxibyp8kv8jhgfvrlcz7z1x>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxibyp8kv8jhgfvrldd4z1>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxibyp8kv8jhgfvrldd4z1>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxibyp8kv8jhgfvrldz8z1>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxibyp8kv8jhgfvrldz8z1j>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxibyp8kv8jhgfvrlej6z1j>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxibyp8kv8jhgfvrlej6z1x>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxibyp8kv8jhgfvrifj_z1j

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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_z1x1

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxibyp8kv8jhgfvrlgt9z1j>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxibyp8kv8jhgfvrlgt9z1x1>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrljm11>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrijlm111>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrijlm21v>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrijlm21v>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrijlm81x>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrijlm81x>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrijlm81x>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrijlm81x>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrlmr19>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrlmr19>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrlmv1p>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrlmv1p>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrijlmy15>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxidyp8kv8jhgfvrijlmy15>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxieyp8kv8jhgfvrijfecg>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxieyp8kv8jhgfvrijnecm>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxigyp8kv8jhgfvrljuchta>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxigyp8kv8jhgfvrljufnta>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxigyp8kv8jhgfvrlptucht>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-pxigyp8kv8jhgfvrlptufnta>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo5cnqeu92fr1mu53zec>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo5cnqeu92fr1mu53zec>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo5cnqeu92fr1mu53zec>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo5cnqeu92fr1mu53zec>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo5cnqeu92fr1mu53zec>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo5cnqeu92fr1mu53zec>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo5cnqeu92fr1mu53zec>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo5cnqeu92fr1mu53zec>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo5cnqeu92fr1mu53zec>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-kfo7cnqeu92fr1me7ksn6>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ievj2zhzi2ecn5>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ievj2zhzi2ecn5>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ievj2zhzi2ecn5>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ievj2zhzi2ecn5>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ievj2zhzi2ecn5>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ievj2zhzi2ecn5>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ievj2zhzi2ecn5>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ievj2zhzi2ecn5>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ievj2zhzi2ecn5>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-iev12zhzi2ecnf>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-iev12zhzi2ecnf>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-iev12zhzi2ecnf>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ievl2zhzi2ecn5>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual 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-ievl2zhzi2ecn5>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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=f77871ff7694ffea381>

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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-ac

Method GET

Parameter x-content-type-options

Attack

Evidence

Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away 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	533
	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.
Solution	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/c5265a3d
CWE Id	693
WASC Id	15
Plugin Id	10021
Informational	
Charset Mismatch	
Description	<p>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.</p> <p>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.</p>
URL	https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fvirtuestech.com
Method	GET

Parameter

Attack

Evidence

Other There was a charset mismatch between the HTTP Header and the XML encoding declaration:
Info [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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

Other There was a charset mismatch between the HTTP Header and the XML encoding declaration:
Info [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%2Fvirtuestech.com>

Method GET

Param

Attack

Eviden

Other

<https://virtuestech.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvirtuestech.com%2Fcategory%2Fwp-json-oembed%2F>

Info [UTF-8] and [null] do not match.

URE

<https://virtuestech.com/wp-json/ceembed/1.0/embed?format=xml&uri=https%3A%2F%2Fvirtuestech.com%2F>

Method GET

Parameter

Attack

Evidence

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%>

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%>

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%>

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%>

Method GET

Parameter

Attack

Attack

Evidence

Other There was a charset mismatch between the HTTP Header and the XML encoding declaration:
Info [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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

Other There was a charset mismatch between the HTTP Header and the XML encoding declaration:
Info [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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

Other There was a charset mismatch between the HTTP Header and the XML encoding declaration:
Info [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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

Other There was a charset mismatch between the HTTP Header and the XML encoding declaration:
Info [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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

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%>

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%>

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%>

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%>

Method GET

Parameter

Attack

Attack

Evidence

Other There was a charset mismatch between the HTTP Header and the XML encoding declaration:
Info [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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

Other There was a charset mismatch between the HTTP Header and the XML encoding declaration:
Info [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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

Other There was a charset mismatch between the HTTP Header and the XML encoding declaration:
Info [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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

Other There was a charset mismatch between the HTTP Header and the XML encoding declaration:
Info [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%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter

Attack

Evidence

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%>

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%>

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%>

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%>

Method GET

Parameter

Attack

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/"], 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}, 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], see evidence field for the suspicious comment/snippet.
URL	https://virtuestech.com/wp-content/plugins/contact-form-7/includes/js/index.js?ver=6.0.6
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.ti 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,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 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%2Fwp-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/
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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/"], 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/ 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	<pre><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-.563.562-1.562-.562-2.063.062l.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><i class="lqd-icn-ess icon-ion-ios-arrow-down"></i></pre>
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-.563.562-1.562-.562-2.063.062l.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><i class="lqd-icn-ess icon-ion-ios-arrow-down"></i>

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 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 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 48-48V80a48 48 0 0 0-48-48z"></path></svg>

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 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>

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

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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 18.375l7.938c.562-.562 1.562-.562
  2.125 0s.562 1.563 0 2.126l-9 9c-.563.562-1.562-1.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL

<https://virtuestech.com/?liquid-header=new-header>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-1.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL

<https://virtuestech.com/?liquid-header=vst-main-header>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-1.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL	https://virtuestech.com/?liquid-mega-menu=cs-menu	
Method	GET	
Parameter		
Attack		
Evidence	 Proactive Defense for a Resilient Digital Future <i aria-hidden="true" class="lqd-icn-ess icon-ion-ios-arrow-forward"></i> 	
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	 Quality Assurance <i aria-hidden="true" class="lqd-icn-ess icon-ion-ios-arrow-forward"></i> 	
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	 Future-Ready Strategies for Unmatched Growth 	
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	<pre> Security advisory <i aria-hidden="true" class="lqd-icn-ess icon-ion-ios-arrow-forward"></i> </pre>
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	<pre> Empower Your Digital Transformation with Flawless Quality </pre>
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	<pre></pre>
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	<pre> Quality Engineering <i aria-hidden="true" class="lqd-icn-ess icon-ion-ios-arrow-forward"></i> </pre>
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 Talent as a service <i aria-hidden="true" class="lqd-icn-ess icon-ion-ios-arrow-forward"></i>

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-.563.562-1.562-.562-2.063.062l.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><i class="lqd-icn-ess icon-ion-ios-arrow-down"></i>

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-.563.562-1.562-.562-2.063.062l.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><i class="lqd-icn-ess icon-ion-ios-arrow-down"></i>

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

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/ai-driven-test-automation-2/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/atlas/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/author/virtuestech/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/best-practices-for-effective-software-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/blogs/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/careers/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/category/cyber-security/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/category/digital-assurance/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/category/quality-engineering/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/category/software-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/category/uncategorized/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/contact/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/cybersecurity-services/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/importance-of-data-loss-prevention-and-why-it-is-requisite-for-any-industry/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/importance-of-performance-testing-and-monitoring/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562 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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/industries/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562 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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/insights/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562 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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/accessibility-usability-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/advisory-and-transformation/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/agile-and-devops-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/ai-driven-test-automation/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/api-security-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/api-testing-services/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/business-experience-validation/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/cloud-native-application-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/cloud-security-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/compliance-and-security-audits/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/comprehensive-test-automation-framework/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/continuous-quality-engineering/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/cyber-resilience-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/data-driven-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/devsecops-integration/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/iot-and-embedded-systems-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/iot-security-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/managed-soc-services/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/manual-testing-services/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/mobile-security-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/penetration-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/performance-engineering-monitoring/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/performance-testing-services>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/secure-code-validation/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/security-audits-and-compliance>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/shift-left-and-shift-right-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/test-center-of-excellence/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/vulnerability-assessment/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/zero-trust-network-assessments/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/tag/automation-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/tag/integration-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/tag/manual-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/tag/software-testing/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562 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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/tag/test-automation/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562 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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/utilizing-mobile-technology-in-the-field/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562 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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/vulnerability-assessments-penetration-testing-cybersecurity/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/what-is-exploratory-testing-why-and-when-do-we-need-it/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/what-is-integration-testing-and-types-approach/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/why-cloud-security-testing-is-essential/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/why-do-the-mobile-manual-test/>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/why-is-independent-software-testing-vital-to-successful-applications-in-any-industry>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL https://virtuestech.com/wp-content/uploads/2021/10/Virtues_BG-e1678973301100.jpg

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/wp-content/uploads/2021/12/VirtuesTech-logo-Footer-1.png>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/wp-content/uploads/2024/09/Image-2@2x.jpg>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/wp-content/uploads/2024/09/VirtuesTech-logo09.png>

Method GET

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562 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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562 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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/ai-driven-test-automation-2/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562 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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/atlas/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/contact/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/accessibility-usability-testing/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/advisory-and-transformation/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/agile-and-devops-testing/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/ai-driven-test-automation/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/api-security-testing/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/api-testing-services/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/business-experience-validation/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/cloud-native-application-testing/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/cloud-security-testing/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/compliance-and-security-audits/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/comprehensive-test-automation-framework/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/continuous-quality-engineering/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/cyber-resilience-testing/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/data-driven-testing/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/devsecops-integration/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/iot-and-embedded-systems-testing/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/iot-security-testing/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/managed-soc-services/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/manual-testing-services/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/mobile-security-testing/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/penetration-testing/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/performance-engineering-monitoring/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/secure-code-validation/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/shift-left-and-shift-right-testing/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/test-center-of-excellence/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/vulnerability-assessment/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL <https://virtuestech.com/services/zero-trust-network-assessments/>

Method POST

Parameter

Attack

```
<a>Quality Engineering<span class="submenu-expander pos-abs"><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-.563.562-1.562-.562-2.063.062l.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></span><span
  class="link-icon d-inline-flex hide-if-empty right-icon"><i class="lqd-icn-ess
  icon-ion-ios-arrow-down"></i></span></a>
```

Other Info Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

Instances 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

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter cache-control

Attack

Evidence

Other
Info

URL

Method GET

Parameter cache-control

Attack

Evidence

Other Info

URL

Method GET

Parameter cache-control

Attack

Evidence

Other Info

URL

Method GET

Parameter cache-control

Attack

Evidence

Other
Info

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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-1%2Fpost-1%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%2Fcategory%2Fcategory-1%2Fpost-1%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%2Fcategory%2Fcategory-1%2Fpost-1%2F>

Method GET

Parameter cache-control

Attack

Evidence

Other Info

URL

Method GET

Parameter cache-control

Attack

Evidence

Other Info

URL

Method GET

Parameter cache-control

Attack

Evidence

Other Info

URL

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

Attack

Evidence

Other Info

URL

<https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter cache-control

Attack

Evidence

Other
Info

URL

Method GET

Parameter cache-control

Attack

Evidence

Other
Info

URL

Method GET

Parameter cache-control

Attack

Evidence

Other Info

URL

Method GET

Parameter cache-control

Attack

Evidence

Other
Info

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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-1%2Fpost-1%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%2Fcategory%2Fcategory-1%2Fpost-1%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%2Fcategory%2Fcategory-1%2Fpost-1%2F>

Method GET

Parameter cache-control

Attack

Evidence

Other Info

URL

Method GET

Parameter cache-control

Attack

Evidence

Other
Info

URL

Method GET

Parameter cache-control

Attack

Evidence

Other
Info

URL

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

Attack

Evidence

Other
Info

URL

<https://virtuestech.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fvirtuestech.com%2Fcategory%2Fcategory-name%2Fpost-name%2F>

Method GET

Parameter cache-control

Attack

Evidence

Other
Info

URL

Method GET

Parameter cache-control

Attack

Evidence

Other
Info

URL

Method GET

Parameter cache-control

Attack

Evidence

Other
Info

URL

Method GET

Parameter cache-control

Attack

Evidence

Other
Info

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%2Fcategory%2Fcategory-name%2Fpost-name%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%2Fcategory%2Fcategory-1%2Fpost-1%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%2Fcategory%2Fcategory-1%2Fpost-1%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%3Fliquic>

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%3Fliquic>

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%3Fliquic>

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%3Fliquic>

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>

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>

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>

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>

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%3Fliquic
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%3Fliquic
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%3Fliquic
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%3Fliquic
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%3Fliquic
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%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-prac%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%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%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%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

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%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%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%2Findex.html
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%2Findex.html
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%2Findex.html
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%2Findex.html
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%2Findex.html

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%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%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%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%2Futilizing-m>

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%2Fvulnerabilities
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-exploit
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-injection
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-computing-is-so-expensive
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-things-go-wrong
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-incorrect>

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-ac

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". https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
Reference	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/login.min.css?ver=6.7.2
Method	GET
Parameter	
Attack	
Evidence	Age: 192196
Other 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: 192197
Other Info	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=6.0.6
Method	GET
Parameter	

Attack

Evidence Age: 291739

Other Info 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=6.0.6>

Method GET

Parameter

Attack

Evidence Age: 291736

Other Info 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: 2540

Other Info 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: 70020

Other Info 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: 2541

Other Info	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: 70020
Other Info	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: 263483
Other Info	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: 263494
Other Info	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: 70019
Other Info	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: 2541
Other Info	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-1.css?ver=6.7.19
Method	GET
Parameter	
Attack	
Evidence	Age: 2543
Other Info	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=6.7.19
Method	GET
Parameter	
Attack	
Evidence	Age: 263494
Other Info	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: 443189
Other Info	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/css/elements/base/typography.css?ver=6.7.19
Method	GET
Parameter	
Attack	

Evidence Age: 2540

Other Info 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: 418898

Other Info 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: 2544

Other Info 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: 263484

Other Info 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: 20174

Other Info 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: 544494	
Other Info	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: 418898	
Other Info	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/ScrollTrigger.min.js	
Method	GET	
Parameter		
Attack		
Evidence	Age: 418898	
Other Info	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: 2541	
Other Info	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: 291738

Other Info 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: 418900

Other Info 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: 263482

Other Info 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: 418898

Other Info 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.js>

Method GET

Parameter

Attack

Evidence Age: 263495

Other Info	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.js
Method	GET
Parameter	
Attack	
Evidence	Age: 443192
Other Info	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: 418898
Other Info	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: 263482
Other Info	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/style.css
Method	GET
Parameter	
Attack	
Evidence	Age: 418899
Other Info	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: 3604
Other Info	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: 360428
Other Info	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: 12
Other Info	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: 1853
Other Info	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: 426

Other Info 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: 249097

Other Info 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: 27

Other Info 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: 26

Other Info 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: 388

Other Info 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.png	
Method	GET	
Parameter		
Attack		
Evidence	Age: 2537	
Other Info	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: 367926	
Other Info	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: 6018	
Other Info	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: 368273	
Other Info	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: 386

Other Info 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: 70008

Other Info 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: 387

Other Info 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: 3546

Other Info 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: 387

Other Info	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: 387
Other Info	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: 6017
Other Info	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: 390
Other Info	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: 360429
Other Info	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: 360436
Other Info	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: 2724
Other Info	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: 383
Other Info	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: 1761
Other Info	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: 3935

Other Info 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: 6017

Other Info 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: 364667

Other Info 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: 3941

Other Info 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-e17297>

Method GET

Parameter

Attack

Evidence Age: 378

Other Info 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: 171901	
Other Info	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-e172976.jpeg	
Method	GET	
Parameter		
Attack		
Evidence	Age: 376	
Other Info	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-e172976.jpeg	
Method	GET	
Parameter		
Attack		
Evidence	Age: 379	
Other Info	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: 382	
Other Info	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: 380

Other Info 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: 376

Other Info 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: 377

Other Info 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: 375

Other Info 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: 385

Other Info	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: 418909
Other Info	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: 320733
Other Info	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-1
Method	GET
Parameter	
Attack	
Evidence	Age: 3939
Other Info	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.j
Method	GET
Parameter	
Attack	
Evidence	Age: 14
Other Info	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: 291725
Other Info	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: 1810
Other Info	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: 263470
Other Info	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: 373
Other Info	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: 169180

Other Info 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: 263486

Other Info 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: 317793

Other Info 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: 263470

Other Info 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: 360433

Other Info 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: 373	
Other Info	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: 171874	
Other Info	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: 253301	
Other Info	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/Underline03.png	
Method	GET	
Parameter		
Attack		
Evidence	Age: 6018	
Other Info	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/aleo.css?ver=1744452449	
Method	GET	
Parameter		

Attack

Evidence Age: 252425

Other Info 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: 2540

Other Info 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: 443191

Other Info 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: 2540

Other Info 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>

Method GET

Parameter

Attack

Evidence Age: 70033

Other Info	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-pxieyp8kv8jhgfvrijfecq.w
Method	GET
Parameter	
Attack	
Evidence	Age: 412878
Other Info	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-kfo7cnqueu92fr1me7ksn6
Method	GET
Parameter	
Attack	
Evidence	Age: 412877
Other 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: 320974
Other 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: 70023
Other 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: 291736

Other 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: 418885

Other 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: 2735

Other Info The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

Instances 102

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

Solution 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-ac

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
Instances	5
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112
Informational	User Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://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

User-controlled HTML 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

User-controlled HTML 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

User-controlled HTML 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

User-controlled HTML 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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info 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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info 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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info 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

User-controlled HTML 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-ac

Method GET

Parameter redirect_to

Attack

Evidence

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:
https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-ac 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-ac

Method GET

Parameter redirect_to

Attack

Evidence

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:
https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-ac 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-ac

Method GET

Parameter redirect_to

Attack

Evidence

Other Info	<p>User-controlled HTML 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/ 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</p>
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin/
Method	GET
Parameter	redirect_to
Attack	
Evidence	
Other Info	<p>User-controlled HTML 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/ 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</p>
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin/
Method	GET
Parameter	redirect_to
Attack	
Evidence	
Other Info	<p>User-controlled HTML 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/ 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</p>
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin/
Method	GET
Parameter	redirect_to
Attack	
Evidence	

Other Info	<p>User-controlled HTML 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/ 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</p>
URL	https://virtuestech.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fvirtuestech.com%2Fwp-admin/
Method	GET
Parameter	redirect_to
Attack	
Evidence	
Other Info	<p>User-controlled HTML 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/ 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</p>
URL	https://virtuestech.com/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	<p>User-controlled HTML 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</p>
URL	https://virtuestech.com/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	<p>User-controlled HTML 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</p>
URL	https://virtuestech.com/
Method	POST

Parameter _wpcf7_container_post

Attack

Evidence

Other User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: <https://virtuestech.com/> appears to include Info 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 User-controlled HTML 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 Info 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 User-controlled HTML 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 Info 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 User-controlled HTML 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 Info 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=6.0.6 The user-controlled value was: 6.0.6
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	<p>User-controlled HTML 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</p>
URL	<p>https://virtuestech.com/ai-driven-test-automation-2/</p>
Method	<p>POST</p>
Parameter	<p>_wpcf7_unit_tag</p>
Attack	
Evidence	
Other Info	<p>User-controlled HTML 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</p>
URL	<p>https://virtuestech.com/ai-driven-test-automation-2/</p>
Method	<p>POST</p>
Parameter	<p>_wpcf7_unit_tag</p>
Attack	
Evidence	
Other Info	<p>User-controlled HTML 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</p>
URL	<p>https://virtuestech.com/ai-driven-test-automation-2/</p>
Method	<p>POST</p>
Parameter	<p>_wpcf7_unit_tag</p>
Attack	
Evidence	
Other Info	<p>User-controlled HTML 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</p>
URL	<p>https://virtuestech.com/ai-driven-test-automation-2/</p>
Method	<p>POST</p>

Parameter _wpcf7_unit_tag

Attack

Evidence

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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=6.0.6 The user-controlled value was: 6.0.6

URL <https://virtuestech.com/ai-driven-test-automation-2/>

Method POST

Parameter email-873

Attack

Evidence

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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=999999999999 The user-controlled value was: 999999999999

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=6.0.6 The user-controlled value was: 6.0.6

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=999999999999 The user-controlled value was: 999999999999

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=6.0.6 The user-controlled value was: 6.0.6

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=999999999999 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	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/accessibility-usability-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6</p>
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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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=6.0.6 The user-controlled value was: 6.0.6

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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6</p>
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/agile-and-devops-testing/

Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/agile-and-devops-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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=6.0.6 The user-controlled value was: 6.0.6

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	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/ai-driven-test-automation/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6

URL <https://virtuestech.com/services/api-security-testing/>

Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/api-security-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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	<p>User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6</p>
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/api-testing-services/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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/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/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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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=6.0.6 The user-controlled value was: 6.0.6

URL

<https://virtuestech.com/services/business-experience-validation/>

Method POST

Parameter email-873

Attack

Evidence

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6

URL <https://virtuestech.com/services/cloud-native-application-testing/>

Method POST

Parameter email-873

Attack

Evidence

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:
<https://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	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/cloud-native-application-testing/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6

URL <https://virtuestech.com/services/cloud-security-testing/>

Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/cloud-security-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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	<p>User-controlled HTML attribute 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</p>
URL	<p>https://virtuestech.com/services/compliance-and-security-audits/</p>
Method	<p>POST</p>
Parameter	<p>_wpcf7_unit_tag</p>
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	<p>https://virtuestech.com/services/compliance-and-security-audits/</p>
Method	<p>POST</p>
Parameter	<p>_wpcf7_unit_tag</p>
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	<p>https://virtuestech.com/services/compliance-and-security-audits/</p>
Method	<p>POST</p>
Parameter	<p>_wpcf7_unit_tag</p>
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	<p>https://virtuestech.com/services/compliance-and-security-audits/</p>

Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6</p>
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/compliance-and-security-audits/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:</p>	
Other Info	<p>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</p>	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/	
Method	POST	
Parameter	_wpcf7_version	
Attack		
Evidence	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:</p>	
Other Info	<p>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=6.0.6 The user-controlled value was: 6.0.6</p>	
URL	https://virtuestech.com/services/comprehensive-test-automation-framework/	
Method	POST	
Parameter	email-873	
Attack		
Evidence	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:</p>	
Other Info	<p>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</p>	
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=999999999999 The user-controlled value was: 999999999999

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	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7_container_post
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/continuous-quality-engineering/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6</p>
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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6

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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6</p>
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/data-driven-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/data-driven-testing/

Method POST

Parameter text-192

Attack

Evidence

Other User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:
Info <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 User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:
Info <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 User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:
Info <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=6.0.6 The user-controlled value was: 6.0.6

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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/iot-and-embedded-systems-testing/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6</p>

URL

<https://virtuestech.com/services/iot-and-embedded-systems-testing/>

Method POST

Parameter email-873

Attack

Evidence

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:
<https://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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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	<p>User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6</p>
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/iot-security-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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/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/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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

Other Info

URL	https://virtuestech.com/services/managed-soc-services/	
Method	POST	
Parameter	_wpcf7_unit_tag	
Attack		
Evidence		
Other Info	<p>User-controlled HTML attribute 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</p>	
URL	https://virtuestech.com/services/managed-soc-services/	
Method	POST	
Parameter	_wpcf7_unit_tag	
Attack		
Evidence		
Other Info	<p>User-controlled HTML attribute 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</p>	
URL	https://virtuestech.com/services/managed-soc-services/	
Method	POST	
Parameter	_wpcf7_unit_tag	
Attack		
Evidence		
Other Info	<p>User-controlled HTML attribute 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</p>	
URL	https://virtuestech.com/services/managed-soc-services/	
Method	POST	
Parameter	_wpcf7_unit_tag	
Attack		
Evidence		

Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6</p>
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/managed-soc-services/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/managed-soc-services/

Method POST

Parameter text-192

Attack

Evidence

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:
<https://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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6

URL <https://virtuestech.com/services/manual-testing-services/>

Method POST

Parameter email-873

Attack

Evidence

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:
<https://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	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/manual-testing-services/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6

URL <https://virtuestech.com/services/mobile-security-testing/>

Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/mobile-security-testing/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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	<p>User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6</p>
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/penetration-testing/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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/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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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=6.0.6 The user-controlled value was: 6.0.6

URL <https://virtuestech.com/services/performance-engineering-monitoring/>

Method POST

Parameter email-873

Attack

Evidence

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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=999999999999 The user-controlled value was: 999999999999

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=6.0.6 The user-controlled value was: 6.0.6

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=999999999999 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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info <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=6.0.6 The user-controlled value was: 6.0.6

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

User-controlled HTML attribute 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

User-controlled HTML attribute 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

User-controlled HTML attribute 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	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6</p>
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/test-center-of-excellence/

Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/test-center-of-excellence/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	_wpcf7
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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=6.0.6 The user-controlled value was: 6.0.6

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	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/vulnerability-assessment/
Method	POST
Parameter	text-438
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7_unit_tag
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	_wpcf7_version
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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=6.0.6 The user-controlled value was: 6.0.6</p>
URL	https://virtuestech.com/services/zero-trust-network-assessments/

Method	POST
Parameter	email-873
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	tel-969
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
URL	https://virtuestech.com/services/zero-trust-network-assessments/
Method	POST
Parameter	text-192
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute 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</p>
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	<p>User-controlled HTML 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</p>
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	user_login
Attack	
Evidence	
Other Info	<p>User-controlled HTML 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</p>
URL	https://virtuestech.com/wp-login.php?action=lostpassword
Method	POST
Parameter	wp-submit
Attack	
Evidence	
Other Info	<p>User-controlled HTML 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</p>
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.

