Virtuelity
Vulnerability Scanner

Vulnerability Scan Report

ZAP by Checkmarx ZAP Scanning Report

Site: https://moxiehawk.com

Generated on Tue, 15 Apr 2025 15:24:05

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	8
Low	4
Informational	3
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	2
CSP: Failure to Define Directive with No Fallback	Medium	27
CSP: Wildcard Directive	Medium	27
CSP: script-src unsafe-inline	Medium	27
CSP: style-src unsafe-inline	Medium	27
Content Security Policy (CSP) Header Not Set	Medium	4

Missing Anti-clickjacking Header	Medium	25
Vulnerable JS Library	Medium	1
Cross-Domain JavaScript Source File Inclusion	Low	29
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	25
Strict-Transport-Security Header Not Set	Low	114
X-Content-Type-Options Header Missing	Low	108
Information Disclosure - Suspicious Comments	Informational	32
Modern Web Application	Informational	11
Re-examine Cache-control Directives	Informational	25

Alert Detail

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://moxiehawk.com/contact.php
Method	GET

		Parameter	
		Attack	
		Evidence	<form id="myForm" 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: "email" "mobile" "name" "subject"].
	URL		https://moxiehawk.com/contact.php
		Method	POST
		Parameter	
		Attack	
		Evidence	<form id="myForm" 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: "email" "mobile" "name" "subject"].
Instances			2

Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet. https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	CSP: Failure to Define Directive with No Fallback
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding them is the same as allowing anything.
URL	https://moxiehawk.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://moxiehawk.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://moxiehawk.com/about.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://moxiehawk.com/apptest.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://moxiehawk.com/blog.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://moxiehawk.com/cloud.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://moxiehawk.com/contact.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://moxiehawk.com/encr.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://moxiehawk.com/host.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://moxiehawk.com/incident.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://moxiehawk.com/index.html
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL		https://moxiehawk.com/index.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://moxiehawk.com/iot.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://moxiehawk.com/net.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://moxiehawk.com/riskassess.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://moxiehawk.com/robots.txt
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL		https://moxiehawk.com/security.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://moxiehawk.com/service.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://moxiehawk.com/soc.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://moxiehawk.com/social.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://moxiehawk.com/source.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://moxiehawk.com/threat.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://moxiehawk.com/tool.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://moxiehawk.com/train.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://moxiehawk.com/vul.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://moxiehawk.com/webtest.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://moxiehawk.com/contact.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.
Instances		27
Solution		Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference		https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_reso
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://moxiehawk.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://moxiehawk.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://moxiehawk.com/about.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://moxiehawk.com/apptest.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://moxiehawk.com/blog.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://moxiehawk.com/cloud.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://moxiehawk.com/contact.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://moxiehawk.com/encr.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://moxiehawk.com/host.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://moxiehawk.com/incident.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://moxiehawk.com/index.html
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL		https://moxiehawk.com/index.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://moxiehawk.com/iot.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://moxiehawk.com/net.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://moxiehawk.com/riskassess.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://moxiehawk.com/robots.txt
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
URL		https://moxiehawk.com/security.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://moxiehawk.com/service.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://moxiehawk.com/soc.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://moxiehawk.com/social.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://moxiehawk.com/source.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://moxiehawk.com/threat.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://moxiehawk.com/tool.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://moxiehawk.com/train.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://moxiehawk.com/vul.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://moxiehawk.com/webtest.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://moxiehawk.com/contact.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
Instances		27
Solution		Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference		https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_reso
CWE Id		693
WASC Id		15
Plugin Id		10055
Medium		**CSP: script-src unsafe-inline**
Description		Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL		https://moxiehawk.com
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests

	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/about.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/apptest.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/blog.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/cloud.php

	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/contact.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/encr.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/host.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/incident.php
	Method	GET
	Parameter	content-security-policy
	Attack	

	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/index.html
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/index.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/iot.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/net.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.

URL		https://moxiehawk.com/riskassess.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/robots.txt
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/security.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/service.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/soc.php
	Method	GET
	Parameter	content-security-policy

	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/social.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/source.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/threat.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/tool.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests

	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/train.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/vul.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/webtest.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
URL		https://moxiehawk.com/contact.php
	Method	POST
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	script-src includes unsafe-inline.
Instances		27

Solution		Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference		https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_reso
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://moxiehawk.com
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/about.php
	Method	GET

	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/apptest.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/blog.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/cloud.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/contact.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests

	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/encr.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/host.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/incident.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/index.html
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/index.php

	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/iot.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/net.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/riskassess.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/robots.txt
	Method	GET
	Parameter	content-security-policy
	Attack	

	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/security.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/service.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/soc.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/social.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.

URL		https://moxiehawk.com/source.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/threat.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/tool.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/train.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/vul.php
	Method	GET
	Parameter	content-security-policy

	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/webtest.php
	Method	GET
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
URL		https://moxiehawk.com/contact.php
	Method	POST
	Parameter	content-security-policy
	Attack	
	Evidence	upgrade-insecure-requests
	Other Info	style-src includes unsafe-inline.
Instances		27
Solution		Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference		https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_reso
CWE Id		693
WASC Id		15
Plugin Id		10055
Medium		**Content Security Policy (CSP) Header Not Set**

Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://moxiehawk.com/apptest.app
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://moxiehawk.com/assets/img/home-six/banner/banner-img.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://moxiehawk.com/privacy-policy.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://moxiehawk.com/terms-conditions.html
Method	GET
Parameter	
Attack	
Evidence	

	Other Info	
Instances		4
Solution		Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference		https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id		693
WASC Id		15
Plugin Id		10038
Medium		**Missing Anti-clickjacking Header**
Description		The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL		https://moxiehawk.com
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/about.php
	Method	GET

	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/apptest.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/blog.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/cloud.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/contact.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	

	Other Info	
URL		https://moxiehawk.com/encr.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/host.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/incident.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/index.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/iot.php

	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/net.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/riskassess.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/security.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/service.php
	Method	GET
	Parameter	x-frame-options
	Attack	

	Evidence	
	Other Info	
URL		https://moxiehawk.com/soc.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/social.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/source.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/threat.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	

URL		https://moxiehawk.com/tool.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/train.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/vul.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/webtest.php
	Method	GET
	Parameter	x-frame-options
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/contact.php
	Method	POST
	Parameter	x-frame-options

	Attack	
	Evidence	
	Other Info	
Instances		25
Solution		Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference		https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id		1021
WASC Id		15
Plugin Id		10020
Medium		**Vulnerable JS Library**
Description		The identified library appears to be vulnerable.
URL		https://moxiehawk.com/assets/js/bootstrap.min.js
	Method	GET
	Parameter	
	Attack	
	Evidence	* Bootstrap v4.5.2
	Other Info	The identified library bootstrap, version 4.5.2 is vulnerable. CVE-2024-6531 https://www.herodevs.com/vulnerability-directory/cve-2024-6531 https://github.com/advisories/GHSA-vc8w-jr9v-vj7f https://nvd.nist.gov/vuln/detail/CVE-2024-6531 https://github.com/rubysec/ruby-advisory-db/blob/master/gems/bootstrap/CVE-2024-6531.yml https://github.com/twbs/bootstrap
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	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://moxiehawk.com
Method	GET
Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
Attack	
Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
Other Info	
URL	https://moxiehawk.com/
Method	GET
Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
Attack	
Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
Other Info	
URL	https://moxiehawk.com/about.php
Method	GET
Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
Attack	
Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
Other Info	
URL	https://moxiehawk.com/apptest.php
Method	GET
Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
Attack	
Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
Other Info	

URL		https://moxiehawk.com/blog.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/cloud.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/contact.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/contact.php
	Method	GET
	Parameter	https://www.google.com/recaptcha/api.js
	Attack	
	Evidence	<script src="https://www.google.com/recaptcha/api.js"></script>
	Other Info	
URL		https://moxiehawk.com/contact.php
	Method	GET
	Parameter	https://www.google.com/recaptcha/api.js?render=6LdU4Q4aAAAAAMF3ZVtqsfoamhdMk2xM7P6RAbJR

	Attack	
	Evidence	<script src="https://www.google.com/recaptcha/api.js?render=6LdU4Q4aAAAAAMF3ZVtqsfoamhdMk2xM7P6RA
	Other Info	
URL		https://moxiehawk.com/encr.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/host.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/incident.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/index.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>

	Other Info	
URL		https://moxiehawk.com/iot.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/net.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/riskassess.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/security.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/service.php

	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/soc.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/social.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/source.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/threat.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	

	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/tool.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/train.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/vul.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/webtest.php
	Method	GET
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	

URL		https://moxiehawk.com/contact.php
	Method	POST
	Parameter	https://code.iconify.design/1/1.0.7/iconify.min.js
	Attack	
	Evidence	<script src="https://code.iconify.design/1/1.0.7/iconify.min.js"></script>
	Other Info	
URL		https://moxiehawk.com/contact.php
	Method	POST
	Parameter	https://www.google.com/recaptcha/api.js
	Attack	
	Evidence	<script src="https://www.google.com/recaptcha/api.js"></script>
	Other Info	
URL		https://moxiehawk.com/contact.php
	Method	POST
	Parameter	https://www.google.com/recaptcha/api.js?render=6LdU4Q4aAAAAAMF3ZVtqsfoamhdMk2xM7P6RAbJR
	Attack	
	Evidence	<script src="https://www.google.com/recaptcha/api.js?render=6LdU4Q4aAAAAAMF3ZVtqsfoamhdMk2xM7P6RA
	Other Info	
Instances		29
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://moxiehawk.com
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/about.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/apptest.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/blog.php
	Method	GET

	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/cloud.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/contact.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/encr.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/host.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33

	Other Info	
URL		https://moxiehawk.com/incident.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/index.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/iot.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/net.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/riskassess.php

	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/security.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/service.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/soc.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/social.php
	Method	GET
	Parameter	
	Attack	

	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/source.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/threat.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/tool.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	
URL		https://moxiehawk.com/train.php
	Method	GET
	Parameter	
	Attack	
	Evidence	x-powered-by: PHP/7.4.33
	Other Info	

URL	https://moxiehawk.com/vul.php
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/7.4.33
Other Info	
URL	https://moxiehawk.com/webtest.php
Method	GET
Parameter	
Attack	
Evidence	x-powered-by: PHP/7.4.33
Other Info	
URL	https://moxiehawk.com/contact.php
Method	POST
Parameter	
Attack	
Evidence	x-powered-by: PHP/7.4.33
Other Info	
Instances	25
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-In 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://moxiehawk.com
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/1.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/12.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	

URL		https://moxiehawk.com/13.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/2.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/about.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/apptest.app
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/apptest.php
	Method	GET
	Parameter	

	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/css/animate.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/css/bootstrap.min.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/css/boxicons.min.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/css/flaticon.css
	Method	GET
	Parameter	
	Attack	
	Evidence	

	Other Info	
URL		https://moxiehawk.com/assets/css/magnific-popup.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/css/meanmenu.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/css/nice-select.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/css/odometer.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/css/owl.carousel.min.css

	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/css/owl.theme.default.min.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/css/responsive.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/css/style.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/img/favicon.png
	Method	GET
	Parameter	
	Attack	

	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/img/home-six/banner/banner-img.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/img/home-six/banner/shape-1.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/img/home-six/banner/shape-2.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/img/home-six/services/auto.jpg
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	

URL	https://moxiehawk.com/assets/img/home-six/services/confi.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://moxiehawk.com/assets/img/home-six/services/profi.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://moxiehawk.com/assets/img/icon.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://moxiehawk.com/assets/img/key.jpg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://moxiehawk.com/assets/img/logo2.png
Method	GET
Parameter	

	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/img/shape/6.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/img/team/profile.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/img/team/woman.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/js/bootstrap.min.js
	Method	GET
	Parameter	
	Attack	
	Evidence	

	Other Info	
URL		https://moxiehawk.com/assets/js/contact-form-script.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/js/custom.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/js/form-validator.min.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/js/jquery-3.5.1.slim.min.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/js/jquery.ajaxchimp.min.js

	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/js/jquery.appear.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/js/jquery.magnific-popup.min.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/js/jquery.meanmenu.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/js/jquery.nice-select.min.js
	Method	GET
	Parameter	
	Attack	

	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/js/odometer.min.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/js/owl.carousel.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/js/parallax.min.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/assets/js/popper.min.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	

URL		https://moxiehawk.com/assets/js/wow.min.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/blog.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/cloud.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/contact.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/encr.php
	Method	GET
	Parameter	

	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/host.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/htdocs_error/something-lost.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/htdocs_error/style.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/1.%20Networking.png
	Method	GET
	Parameter	
	Attack	
	Evidence	

	Other Info	
URL		https://moxiehawk.com/icon/10.%20Network%20Penetration%20Testing.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/11.%20Web%20Application%20Penetration%20Testing.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/12.%20API%20Penetration%20Testing.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/13.%20Android%20Penetration%20Testing.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/14.%20iOS%20Penetration%20Testing.png

	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/15.%20IOT%20Penetration%20Testing.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/16.%20Cloud%20Assessment.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/17.%20Bug%20Bounty.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/18.%20Malware%20Analysis.png
	Method	GET
	Parameter	
	Attack	

	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/19.%20Reverse%20Engineering.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/2.%20Network%20Security.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/20.%20Tools.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/21.%20Resources.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	

URL		https://moxiehawk.com/icon/22.%20Certificate.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/3.%20Windows.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/4.%20Windows%20Server.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/5.%20Linux.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/6.%20Linux%20Administrator.png
	Method	GET
	Parameter	

	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/7.%20Bash.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/8.%20Python.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/9.%20SQL.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/bugbounty.png
	Method	GET
	Parameter	
	Attack	
	Evidence	

	Other Info	
URL		https://moxiehawk.com/icon/Continuous%20Monitoring.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/Cyber%20Update.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/Data%20Privacy.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/Detailed%20Audit%20Report.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/Incident%20Response.png

	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/Monthly%20Report.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/Offensive%20Methodology.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/offensivetrain.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/penetration.png
	Method	GET
	Parameter	
	Attack	

	Evidence	
	Other Info	
URL		https://moxiehawk.com/icon/Red%20Team.png
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/incident.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/index.html
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/index.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	

URL		https://moxiehawk.com/iot.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/net.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/privacy-policy.html
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/ps-0.9.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/riskassess.php
	Method	GET
	Parameter	

	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/robots.txt
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/scan/assets/css/scan.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/scan/assets/js/scan.js
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/security.php
	Method	GET
	Parameter	
	Attack	
	Evidence	

	Other Info	
URL		https://moxiehawk.com/service.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/sitemap.xml
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/slide.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/soc.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/social.php

	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/source.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/terms-conditions.html
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/threat.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/tool.php
	Method	GET
	Parameter	
	Attack	

	Evidence	
	Other Info	
URL		https://moxiehawk.com/train.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/vul.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/webtest.php
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/contact.php
	Method	POST
	Parameter	
	Attack	
	Evidence	
	Other Info	

Instances	114
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035
Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://moxiehawk.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://moxiehawk.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://moxiehawk.com/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://moxiehawk.com/12.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://moxiehawk.com/13.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://moxiehawk.com/2.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://moxiehawk.com/about.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://moxiehawk.com/apptest.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://moxiehawk.com/assets/css/animate.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://moxiehawk.com/assets/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://moxiehawk.com/assets/css/boxicons.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://moxiehawk.com/assets/css/flaticon.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://moxiehawk.com/assets/css/magnific-popup.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://moxiehawk.com/assets/css/meanmenu.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://moxiehawk.com/assets/css/nice-select.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://moxiehawk.com/assets/css/odometer.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://moxiehawk.com/assets/css/owl.carousel.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://moxiehawk.com/assets/css/owl.theme.default.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://moxiehawk.com/assets/css/responsive.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://moxiehawk.com/assets/css/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://moxiehawk.com/assets/img/favicon.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://moxiehawk.com/assets/img/home-six/banner/shape-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://moxiehawk.com/assets/img/home-six/banner/shape-2.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://moxiehawk.com/assets/img/home-six/services/auto.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://moxiehawk.com/assets/img/home-six/services/confi.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://moxiehawk.com/assets/img/home-six/services/profi.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://moxiehawk.com/assets/img/icon.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://moxiehawk.com/assets/img/key.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://moxiehawk.com/assets/img/logo2.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://moxiehawk.com/assets/img/shape/6.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://moxiehawk.com/assets/img/team/profile.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://moxiehawk.com/assets/img/team/woman.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://moxiehawk.com/assets/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://moxiehawk.com/assets/js/contact-form-script.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://moxiehawk.com/assets/js/custom.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://moxiehawk.com/assets/js/form-validator.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://moxiehawk.com/assets/js/jquery-3.5.1.slim.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://moxiehawk.com/assets/js/jquery.ajaxchimp.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://moxiehawk.com/assets/js/jquery.appear.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://moxiehawk.com/assets/js/jquery.magnific-popup.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://moxiehawk.com/assets/js/jquery.meanmenu.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://moxiehawk.com/assets/js/jquery.nice-select.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://moxiehawk.com/assets/js/odometer.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://moxiehawk.com/assets/js/owl.carousel.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://moxiehawk.com/assets/js/parallax.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://moxiehawk.com/assets/js/popper.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://moxiehawk.com/assets/js/wow.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://moxiehawk.com/blog.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://moxiehawk.com/cloud.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://moxiehawk.com/contact.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://moxiehawk.com/encr.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://moxiehawk.com/host.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://moxiehawk.com/htdocs_error/something-lost.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://moxiehawk.com/htdocs_error/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://moxiehawk.com/icon/1.%20Networking.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://moxiehawk.com/icon/10.%20Network%20Penetration%20Testing.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://moxiehawk.com/icon/11.%20Web%20Application%20Penetration%20Testing.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://moxiehawk.com/icon/12.%20API%20Penetration%20Testing.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://moxiehawk.com/icon/13.%20Android%20Penetration%20Testing.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://moxiehawk.com/icon/14.%20iOS%20Penetration%20Testing.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://moxiehawk.com/icon/15.%20IOT%20Penetration%20Testing.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://moxiehawk.com/icon/16.%20Cloud%20Assessment.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://moxiehawk.com/icon/17.%20Bug%20Bounty.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://moxiehawk.com/icon/18.%20Malware%20Analysis.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://moxiehawk.com/icon/19.%20Reverse%20Engineering.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://moxiehawk.com/icon/2.%20Network%20Security.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://moxiehawk.com/icon/20.%20Tools.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://moxiehawk.com/icon/21.%20Resources.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://moxiehawk.com/icon/22.%20Certificate.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://moxiehawk.com/icon/3.%20Windows.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://moxiehawk.com/icon/4.%20Windows%20Server.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://moxiehawk.com/icon/5.%20Linux.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://moxiehawk.com/icon/6.%20Linux%20Administrator.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://moxiehawk.com/icon/7.%20Bash.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://moxiehawk.com/icon/8.%20Python.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://moxiehawk.com/icon/9.%20SQL.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://moxiehawk.com/icon/bugbounty.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://moxiehawk.com/icon/Continuous%20Monitoring.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://moxiehawk.com/icon/Cyber%20Update.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://moxiehawk.com/icon/Data%20Privacy.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://moxiehawk.com/icon/Detailed%20Audit%20Report.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://moxiehawk.com/icon/Incident%20Response.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://moxiehawk.com/icon/Monthly%20Report.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://moxiehawk.com/icon/Offensive%20Methodology.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://moxiehawk.com/icon/offensivetrain.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://moxiehawk.com/icon/penetration.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://moxiehawk.com/icon/Red%20Team.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://moxiehawk.com/incident.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://moxiehawk.com/index.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://moxiehawk.com/iot.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://moxiehawk.com/net.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://moxiehawk.com/ps-0.9.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://moxiehawk.com/riskassess.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://moxiehawk.com/scan/assets/css/scan.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://moxiehawk.com/scan/assets/js/scan.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://moxiehawk.com/security.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://moxiehawk.com/service.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://moxiehawk.com/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://moxiehawk.com/slide.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://moxiehawk.com/soc.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://moxiehawk.com/social.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://moxiehawk.com/source.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://moxiehawk.com/threat.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://moxiehawk.com/tool.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://moxiehawk.com/train.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://moxiehawk.com/vul.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://moxiehawk.com/webtest.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://moxiehawk.com/contact.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.
Instances		108
Solution		Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Reference		https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g https://owasp.org/www-community/Security_Headers
CWE Id		693
WASC Id		15
Plugin Id		10021
Informational		**Information Disclosure - Suspicious Comments**

Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://moxiehawk.com/assets/js/custom.js
Method	GET
Parameter	
Attack	
Evidence	Select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "// Nice Select JS", see evidence field for the suspicious comment/snippet.
URL	https://moxiehawk.com/assets/js/jquery-3.5.1.slim.min.js
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//,Rt={},Mt={},It="*/".concat("*"),Wt=E.createElement("a");function Ft(o){return function(e,t){"string"!=typeof e&&(t=e,e="*");v", see evidence field for the suspicious comment/snippet.
URL	https://moxiehawk.com/assets/js/jquery.nice-select.min.js
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//github.com/hernansartorio/jquery-nice-select", see evidence field for the suspicious comment/snippet.
URL	https://moxiehawk.com/assets/js/owl.carousel.js
Method	GET
Parameter	
Attack	
Evidence	TODO

	Other Info	The following pattern was used: \bTODO\b and was detected in likely comment: "// TODO: Should be computed from number of min width items in stage", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/scan/assets/js/scan.js
	Method	GET
	Parameter	
	Attack	
	Evidence	select
	Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//scan/assets/packs/",n(n.s=1350)}({1345:function(e,t,n){var r={};function i(e){var t=a(e);return n(t)}function a(e){if(!n.o(r,e", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/about.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Bug
	Other Info	The following pattern was used: \bBUG\b and was detected in likely comment: "<!-- <span>OSCP | CEH | Penetration Tester | Security Researcher | Bug Hunter | Python Developer | Malware Analyst</s", see evidence field for the suspicious comment/snippet.

URL		https://moxiehawk.com/about.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/apptest.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/blog.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/cloud.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/contact.php
	Method	GET
	Parameter	

	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/encr.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/host.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/incident.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/index.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select

	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/iot.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/net.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/riskassess.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/security.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/service.php

	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/soc.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/social.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/source.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/threat.php
	Method	GET
	Parameter	
	Attack	

	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/tool.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/train.php
	Method	GET
	Parameter	
	Attack	
	Evidence	from
	Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "<!--Animation Scannner Start from Here -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/train.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/vul.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.

URL		https://moxiehawk.com/webtest.php
	Method	GET
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
URL		https://moxiehawk.com/contact.php
	Method	POST
	Parameter	
	Attack	
	Evidence	Select
	Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in likely comment: "<!-- Nice Select CSS -->", see evidence field for the suspicious comment/snippet.
Instances		32
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://moxiehawk.com
	Method	GET
	Parameter	
	Attack	
	Evidence	<a href="#"> Reconnaissance </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://moxiehawk.com/

	Method	GET
	Parameter	
	Attack	
	Evidence	<a href="#"> Reconnaissance </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://moxiehawk.com/about.php
	Method	GET
	Parameter	
	Attack	
	Evidence	<a href="#"> Autonomy </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://moxiehawk.com/apptest.app
	Method	GET
	Parameter	
	Attack	
	Evidence	<script> (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','https://www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-26575989-46', 'auto'); ga('send', 'pageview'); </script>
	Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL		https://moxiehawk.com/assets/img/home-six/banner/banner-img.png
	Method	GET
	Parameter	
	Attack	
	Evidence	<script> (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','https://www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-26575989-46', 'auto'); ga('send', 'pageview'); </script>
	Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.

<table>
<tr><td>URL</td><td></td><td>https://moxiehawk.com/index.html</td></tr>
<tr><td></td><td>Method</td><td>GET</td></tr>
<tr><td></td><td>Parameter</td><td></td></tr>
<tr><td></td><td>Attack</td><td></td></tr>
<tr><td></td><td>Evidence</td><td><script> (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','https://www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-26575989-46', 'auto'); ga('send', 'pageview'); </script></td></tr>
<tr><td></td><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr>
<tr><td>URL</td><td></td><td>https://moxiehawk.com/index.php</td></tr>
<tr><td></td><td>Method</td><td>GET</td></tr>
<tr><td></td><td>Parameter</td><td></td></tr>
<tr><td></td><td>Attack</td><td></td></tr>
<tr><td></td><td>Evidence</td><td><a href="#"> Reconnaissance </a></td></tr>
<tr><td></td><td>Other Info</td><td>Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.</td></tr>
<tr><td>URL</td><td></td><td>https://moxiehawk.com/privacy-policy.html</td></tr>
<tr><td></td><td>Method</td><td>GET</td></tr>
<tr><td></td><td>Parameter</td><td></td></tr>
<tr><td></td><td>Attack</td><td></td></tr>
<tr><td></td><td>Evidence</td><td><script> (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','https://www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-26575989-46', 'auto'); ga('send', 'pageview'); </script></td></tr>
<tr><td></td><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr>
<tr><td>URL</td><td></td><td>https://moxiehawk.com/robots.txt</td></tr>
<tr><td></td><td>Method</td><td>GET</td></tr>
<tr><td></td><td>Parameter</td><td></td></tr>
<tr><td></td><td>Attack</td><td></td></tr>
</table>

Evidence	<script> (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','https://www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-26575989-46', 'auto'); ga('send', 'pageview'); </script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://moxiehawk.com/terms-conditions.html
Method	GET
Parameter	
Attack	
Evidence	<script> (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','https://www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-26575989-46', 'auto'); ga('send', 'pageview'); </script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://moxiehawk.com/train.php
Method	GET
Parameter	
Attack	
Evidence	<a href="#" class="MobileMenuIcon" id="js-mobile-menu-icon" aria-haspopup="true" aria-expanded="false" aria-controls="js-mobile-menu" aria-label=”Mobile navigation menu”> </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	11
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	[10109](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://moxiehawk.com
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/about.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/apptest.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/blog.php
	Method	GET
	Parameter	cache-control

	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/cloud.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/contact.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/encr.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/host.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	

	Other Info	
URL		https://moxiehawk.com/incident.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/index.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/iot.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/net.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/riskassess.php

	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/security.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/service.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/sitemap.xml
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/soc.php
	Method	GET
	Parameter	cache-control
	Attack	

	Evidence	
	Other Info	
URL		https://moxiehawk.com/social.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/source.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/threat.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/tool.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	

URL		https://moxiehawk.com/train.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/vul.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
URL		https://moxiehawk.com/webtest.php
	Method	GET
	Parameter	cache-control
	Attack	
	Evidence	
	Other Info	
Instances		25
Solution		For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference		https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-c 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

Sequence Details

With the associated active scan results.

Report generated by VirtuesTech Security Scanner

Virtuelity

Vulnerability Scanner