ZAP Scanning Report

Site: https://ascii-docs.web.app

Generated on Sun, 19 Dec 2021 20:24:47

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	4
Informational	1

Alerts

Name	Risk Level	Number of Instances
Application Error Disclosure	Medium	1
X-Frame-Options Header Not Set	Medium	5
Absence of Anti-CSRF Tokens	Low	22
Incomplete or No Cache-control Header Set	Low	5
Timestamp Disclosure - Unix	Low	10
X-Content-Type-Options Header Missing	Low	9
Information Disclosure - Suspicious Comments	Informational	8

Alert Detail

Medium	Application Error Disclosure
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	invalid query
Instances	1
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	90022

Medium	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://ascii-docs.web.app
Method	GET
Attack	
Evidence	
URL	https://ascii-docs.web.app/
Method	GET
Attack	
Evidence	
URL	https://ascii-docs.web.app/css
Method	GET
Attack	
Evidence	
URL	https://ascii-docs.web.app/robots.txt
Method	GET
Attack	
Evidence	
URL	https://ascii-docs.web.app/sitemap.xml
Method	GET
Attack	
Evidence	
Instances	5
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (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

Low	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://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET

Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	

Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	<form onsubmit="return false;">
Instances	22
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	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Low	Incomplete or No Cache-control Header Set
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content.
URL	https://ascii-docs.web.app
Method	GET
Attack	
Evidence	max-age=3600
URL	https://ascii-docs.web.app/
Method	GET
Attack	
Evidence	max-age=3600
URL	https://ascii-docs.web.app/css
Method	GET
Attack	
Evidence	max-age=3600
URL	https://ascii-docs.web.app/robots.txt
Method	GET
Attack	
Evidence	max-age=3600
URL	https://ascii-docs.web.app/sitemap.xml
Method	GET
Attack	
Evidence	max-age=3600
Instances	5
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
CWE Id	525
WASC Id	13
Plugin Id	10015

Low	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	10485760
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	1073741823
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js

Method	GET
Attack	
Evidence	1518500249
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	16711680
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	16777215
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	16777216
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	1732584193
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	1859775393
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	2147483647
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	271733878
Instances	10
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
	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

Description	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://ascii-docs.web.app
Method	GET
Attack	
Evidence	
URL	https://ascii-docs.web.app/
Method	GET
Attack	
Evidence	
URL	https://ascii-docs.web.app/css
Method	GET
Attack	
Evidence	
URL	https://ascii-docs.web.app/css/app.df92db4b.css
Method	GET
Attack	
Evidence	
URL	https://ascii-docs.web.app/css/chunk-vendors.1706ca10.css
Method	GET
Attack	
Evidence	
URL	https://ascii-docs.web.app/js/app.da87ae8a.js
Method	GET
Attack	
Evidence	
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	
URL	https://ascii-docs.web.app/robots.txt
Method	GET
Attack	
Evidence	
URL	https://ascii-docs.web.app/sitemap.xml
Method	GET
Attack	
Evidence	
Instances	9
	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

Solution	If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx 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. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://ascii-docs.web.app/js/app.da87ae8a.js
Method	GET
Attack	
Evidence	query
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	admin
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	db
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	from
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	query
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	SELECT
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	
Evidence	user
URL	https://ascii-docs.web.app/js/chunk-vendors.d57091b8.js
Method	GET
Attack	

Evidence	where
Instances	8
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	[200]()
WASC Id	13
Plugin Id	[10027]()