OWASP ZAP Scan Report

Target: https://taisen.pages.dev

All scanned sites: https://taisen.pages.dev

Javascript included from: https://www.gstatic.com https://cdnjs.cloudflare.com https://cse.google.com https://taisen.pages.dev

Generated on Tue, 7 Oct 2025 14:02:17

ZAP Version: 2.16.1

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	26
Cross-Domain Misconfiguration	Medium	46
Cross-Domain JavaScript Source File Inclusion	Low	4
Re-examine Cache-control Directives	Informational	18

Passing Rules

Name	Rule Type	Threshold	Strength
Session Management Response Identified	Passive	MEDIUM	-
Verification Request Identified	Passive	MEDIUM	-
Private IP Disclosure	Passive	MEDIUM	-
Session ID in URL Rewrite	Passive	MEDIUM	-
Script Served From Malicious Domain (polyfill)	Passive	MEDIUM	-
ZAP is Out of Date	Passive	MEDIUM	-
Insecure JSF ViewState	Passive	MEDIUM	-
Vulnerable JS Library (Powered by Retire.js)	Passive	MEDIUM	-
Charset Mismatch	Passive	MEDIUM	-
Cookie No HttpOnly Flag	Passive	MEDIUM	-
Cookie Without Secure Flag	Passive	MEDIUM	-

Generated by HostedScan

Content-Type Header Missing	Passive	MEDIUM	-
Anti-clickjacking Header	Passive	MEDIUM	-
X-Content-Type-Options Header Missing	Passive	MEDIUM	-
Application Error Disclosure	Passive	MEDIUM	-
Information Disclosure - Debug Error Messages	Passive	MEDIUM	-
Information Disclosure - Sensitive Information in URL	Passive	MEDIUM	-
Information Disclosure - Sensitive Information in HTTP Referrer Header	Passive	MEDIUM	-
Information Disclosure - Suspicious Comments	Passive	MEDIUM	-
Off-site Redirect	Passive	MEDIUM	-
Cookie Poisoning	Passive	MEDIUM	-
User Controllable Charset	Passive	MEDIUM	-
WSDL File Detection	Passive	MEDIUM	-
User Controllable HTML Element Attribute (Potential XSS)	Passive	MEDIUM	-
Loosely Scoped Cookie	Passive	MEDIUM	-
Viewstate	Passive	MEDIUM	-
Directory Browsing	Passive	MEDIUM	-
Heartbleed OpenSSL Vulnerability (Indicative)	Passive	MEDIUM	-
Strict-Transport-Security Header	Passive	MEDIUM	-
HTTP Server Response Header	Passive	MEDIUM	-
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Passive	MEDIUM	-
X-Backend-Server Header Information Leak	Passive	MEDIUM	-
Secure Pages Include Mixed Content	Passive	MEDIUM	-
HTTP to HTTPS Insecure Transition in Form Post	Passive	MEDIUM	-
HTTPS to HTTP Insecure Transition in Form Post	Passive	MEDIUM	-
User Controllable JavaScript Event (XSS)	Passive	MEDIUM	-
Big Redirect Detected (Potential Sensitive Information Leak)	Passive	MEDIUM	-
Retrieved from Cache	Passive	MEDIUM	-
X-ChromeLogger-Data (XCOLD) Header Information Leak	Passive	MEDIUM	-
Cookie without SameSite Attribute	Passive	MEDIUM	-
CSP	Passive	MEDIUM	-
X-Debug-Token Information Leak	Passive	MEDIUM	-
Username Hash Found	Passive	MEDIUM	-
X-AspNet-Version Response Header	Passive	MEDIUM	-
PII Disclosure	Passive	MEDIUM	-
Script Passive Scan Rules	Passive	MEDIUM	-
Stats Passive Scan Rule	Passive	MEDIUM	-
Absence of Anti-CSRF Tokens	Passive	MEDIUM	-
Timestamp Disclosure	Passive	MEDIUM	-
Hash Disclosure	Passive	MEDIUM	-
Weak Authentication Method	Passive	MEDIUM	-
Reverse Tabnabbing	Passive	MEDIUM	-
Modern Web Application	Passive	MEDIUM	-
Authentication Request Identified	Passive	MEDIUM	-

Alert Detail

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://taisen.pages.dev/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Request Header	GET https://taisen.pages.dev/ HTTP/1.1 host: taisen.pages.dev user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 07 Oct 2025 14:01:44 GMT Content-Type: text/html; charset=utf-8 Content-Length: 85828 Connection: keep-alive Access-Control-Allow-Origin: * Cache-Control: public, max-age=31536000 ETag: "8f04b146fcd22dfff6371f09202d0825" Strict-Transport-Security: max-age=63072000; includeSubDomains; preload referrer-policy: no-referrer-when-downgrade x-content-type-options: nosniff x-frame-options: SAMEORIGIN Vary: accept-encoding Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=FRMUV3HETthqUZPlWw%2FPa1o3U7Xfs438JwMR7rNgft3b2wcGQS9k6ogm33N8DU0IDn71uxr9NUTPIeyUt9442WgRZolZpeDGZV%2Fd8G4vlkU%3D"}]} Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800} Server: cloudflare CF-RAY: 98adeea23d6406ee-ATL alt-svc: h3=":443"; ma=86400

Response Body **(truncated)**	<!DOCTYPE html>
	<html lang="en">
	<head>
	  <meta charset="UTF-8">
	  <meta name="viewport" content="width=device-width, initial-scale=1.0">
	  <title>Taisen</title>
	  <link rel="icon" type="image/png" href="original.png">
	  <link rel="stylesheet" href="style.css?v=20250901">
	
	  <!-- Analytics Check - Must be first -->
	  <script>
	    // Check analytics setting before loading anything
	    (function() {
	      const analyticsEnabled = localStorage.getItem('analyticsEnabled');
	      // I...(truncated)

URL	https://taisen.pages.dev/$%7Bitem.link%7D
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/about
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/advertising
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/captcha?q=fmbvYyyc
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/compliance
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://taisen.pages.dev/contact.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/controls
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/favicon.ico
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/help%20center
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/help.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/labs
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/overview
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://taisen.pages.dev/policy.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/privacy
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/privacy-policy.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/resources
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/results
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/security
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/subprocessors
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/taisen-security.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/Taisen_Documentation.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/TaisenSearch_Documentation
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/terms
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://taisen.pages.dev/updates
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

Instances	26
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	https://taisen.pages.dev/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

Request Header	`GET https://taisen.pages.dev/ HTTP/1.1`
	`host: taisen.pages.dev`
	`user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36`
	`pragma: no-cache`
	`cache-control: no-cache`

Request Body	

Response Header	`HTTP/1.1 200 OK`
	`Date: Tue, 07 Oct 2025 14:01:44 GMT`
	`Content-Type: text/html; charset=utf-8`
	`Content-Length: 85828`
	`Connection: keep-alive`
	`Access-Control-Allow-Origin: *`
	`Cache-Control: public, max-age=31536000`
	`ETag: "8f04b146fcd22dfff6371f09202d0825"`
	`Strict-Transport-Security: max-age=63072000; includeSubDomains; preload`
	`referrer-policy: no-referrer-when-downgrade`
	`x-content-type-options: nosniff`
	`x-frame-options: SAMEORIGIN`
	`Vary: accept-encoding`
	`Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=FRMUV3HETthqUZPlWw%2FPa1o3U7Xfs438JwMR7rNgft3b2wcGQS9k6ogm33N8DU0IDn71uxr9NUTPIeyUt9442WgRZolZpeDGZV%2Fd8G4vlkU%3D"}]}`
	`Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}`
	`Server: cloudflare`
	`CF-RAY: 98adeea23d6406ee-ATL`
	`alt-svc: h3=":443"; ma=86400`

Response Body **(truncated)**	`<!DOCTYPE html>`
	`<html lang="en">`

```
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Taisen</title>
  <link rel="icon" type="image/png" href="original.png">
  <link rel="stylesheet" href="style.css?v=20250901">

  <!-- Analytics Check - Must be first -->
  <script>
    // Check analytics setting before loading anything
    (function() {
      const analyticsEnabled = localStorage.getItem('analyticsEnabled');
      // I...(truncated)
```

URL	https://taisen.pages.dev/$%7Bitem.link%7D
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/about
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/about.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/advertising
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/advertising.html

Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/captcha.html?q=fmbvYyyc
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/captcha?q=fmbvYyyc
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/compliance
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/compliance.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/contact.html
Method	GET

Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/controls
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/controls.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/favicon.ico
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/help%20center
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/help%20center.html
Method	GET
Parameter	

Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/help.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/index.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/labs
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/labs.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/original.png
Method	GET
Parameter	
Attack	

Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/overview
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/overview.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/policy.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/privacy
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/privacy-policy.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *

Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/privacy.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/resources
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/resources.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/results
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/robots.txt
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk

	somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/security
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/security.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/style.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/style.css?v=20250901
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

URL	https://taisen.pages.dev/subprocessors
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/subprocessors.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/taisen-security.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/Taisen_Documentation.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/TaisenSearch_Documentation
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/TaisenSearch_Documentation.html

Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/terms
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/terms.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/updates
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://taisen.pages.dev/updates.html
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	46
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

	Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://taisen.pages.dev/
Method	GET
Parameter	https://cse.google.com/cse.js?cx=178f66b21f928448b
Attack	
Evidence	<script async src="https://cse.google.com/cse.js?cx=178f66b21f928448b"></script>
Other Info	
Request Header	GET https://taisen.pages.dev/ HTTP/1.1 host: taisen.pages.dev user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 07 Oct 2025 14:01:44 GMT Content-Type: text/html; charset=utf-8 Content-Length: 85828 Connection: keep-alive Access-Control-Allow-Origin: * Cache-Control: public, max-age=31536000 ETag: "8f04b146fcd22dfff6371f09202d0825" Strict-Transport-Security: max-age=63072000; includeSubDomains; preload referrer-policy: no-referrer-when-downgrade x-content-type-options: nosniff x-frame-options: SAMEORIGIN Vary: accept-encoding Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=FRMUV3HETthqUZPlWw%2FPa1o3U7Xfs438JwMR7rNgft3b2wcGQS9k6ogm33N8DU0IDn71uxr9NUTPIeyUt9442WgRZolZpeDGZV%2Fd8G4vlkU%3D"}]} Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800} Server: cloudflare CF-RAY: 98adeea23d6406ee-ATL alt-svc: h3=":443"; ma=86400

Response Body **(excerpt)**	ion" class="mobile-restriction">
	    <h1>Sorry, this website is not available on mobile devices.</h1>
	    <p>Please access Taisen from a desktop or laptop computer for the best experience.</p>
	  </div>
	
	  <!-- Google Custom Search Script -->
	  <script async src="https://cse.google.com/cse.js?cx=178f66b21f928448b"></script>
	
	  <!-- Search Logging JS -->
	  <script>
	    const SHEET_WEB_APP_URL = "https://script.google.com/macros/s/AKfycbye72BaC5itl9lQNV8k8OrO_E4VjdFbqm3quUX6RnS8s9tOE

	_UbvVd8WBPLDhpgUp6W/exec";
	    const CSE_CX = "178f66b21f928448b";
	
	    // Predefi

URL	https://taisen.pages.dev/
Method	GET
Parameter	https://www.gstatic.com/firebasejs/8.10.1/firebase-app.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/8.10.1/firebase-app.js"></script>
Other Info	
URL	https://taisen.pages.dev/
Method	GET
Parameter	https://www.gstatic.com/firebasejs/8.10.1/firebase-firestore.js
Attack	
Evidence	<script src="https://www.gstatic.com/firebasejs/8.10.1/firebase-firestore.js"></script>
Other Info	
URL	https://taisen.pages.dev/results
Method	GET
Parameter	https://cse.google.com/cse.js?cx=178f66b21f928448b
Attack	
Evidence	<script async src="https://cse.google.com/cse.js?cx=178f66b21f928448b"></script>
Other Info	
Instances	4
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

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://taisen.pages.dev/
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
Request Header	GET https://taisen.pages.dev/ HTTP/1.1 host: taisen.pages.dev user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36

	pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Date: Tue, 07 Oct 2025 14:01:44 GMT Content-Type: text/html; charset=utf-8 Content-Length: 85828 Connection: keep-alive Access-Control-Allow-Origin: * Cache-Control: **public, max-age=31536000** ETag: "8f04b146fcd22dfff6371f09202d0825" Strict-Transport-Security: max-age=63072000; includeSubDomains; preload referrer-policy: no-referrer-when-downgrade x-content-type-options: nosniff x-frame-options: SAMEORIGIN Vary: accept-encoding Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=FRMUV3HETthqUZPlWw%2FPa1o3U7Xfs438JwMR7rNgft3b2wcGQS9k6ogm33N8DU0IDn71uxr9NUTPIeyUt9442WgRZolZpeDGZV%2Fd8G4vlkU%3D"}]} Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800} Server: cloudflare CF-RAY: 98adeea23d6406ee-ATL alt-svc: h3=":443"; ma=86400

Response Body **(truncated)**	<!DOCTYPE html>
	<html lang="en">
	<head>
	  <meta charset="UTF-8">
	  <meta name="viewport" content="width=device-width, initial-scale=1.0">
	  <title>Taisen</title>
	  <link rel="icon" type="image/png" href="original.png">
	  <link rel="stylesheet" href="style.css?v=20250901">
	
	  <!-- Analytics Check - Must be first -->
	  <script>
	    // Check analytics setting before loading anything
	    (function() {
	      const analyticsEnabled = localStorage.getItem('analyticsEnabled');
	      // I...(truncated)

URL	https://taisen.pages.dev/about
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/advertising
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/captcha?q=fmbvYyyc
Method	GET

Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/compliance
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/controls
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/help%20center
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/labs
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/overview
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/privacy
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	

URL	https://taisen.pages.dev/resources
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/results
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/security
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/sitemap.xml
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/subprocessors
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/TaisenSearch_Documentation
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/terms
Method	GET
Parameter	cache-control
Attack	

Evidence	public, max-age=31536000
Other Info	
URL	https://taisen.pages.dev/updates
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=31536000
Other Info	
Instances	18
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015