


ZAP by Checkmarx Scanning Report

Generated with  ZAP on Sat 27 Sept 2025, at 19:55:16

ZAP Version: D-2025-09-18

ZAP by [Checkmarx](#)

Contents

- 1. [About This Report](#)
 - 1. [Report Parameters](#)
- 2. [Summaries](#)
 - 1. [Alert Counts by Risk and Confidence](#)
 - 2. [Alert Counts by Site and Risk](#)
 - 3. [Alert Counts by Alert Type](#)
- 3. [Alerts](#)
 - 1. [Risk=Medium, Confidence=High \(2\)](#)
 - 2. [Risk=Medium, Confidence=Medium \(1\)](#)
 - 3. [Risk=Low, Confidence=Medium \(3\)](#)
 - 4. [Risk=Informational, Confidence=Medium \(2\)](#)
- 4. [Appendix](#)
 - 1. [Alert Types](#)

About This Report

Report Parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- <http://www.itsecgames.com>

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Summaries

Alert Counts by Risk and Confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				Total
		User Confirmed	High	Medium	Low	
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	2 (25.0%)	1 (12.5%)	0 (0.0%)	3 (37.5%)
	Low	0 (0.0%)	0 (0.0%)	3 (37.5%)	0 (0.0%)	3 (37.5%)
	Informational	0 (0.0%)	0 (0.0%)	2 (25.0%)	0 (0.0%)	2 (25.0%)
	Total	0 (0.0%)	2 (25.0%)	6 (75.0%)	0 (0.0%)	8 (100%)

Alert Counts by Site and Risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://www.itsecgames.com	0 (0)	3 (3)	3 (6)	2 (8)

Alert Counts by Alert Type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	7 (87.5%)
Missing Anti-clickjacking Header	Medium	5 (62.5%)
Sub Resource Integrity Attribute Missing	Medium	5 (62.5%)
Insufficient Site Isolation Against Spectre Vulnerability	Low	46 (575.0%)
Permissions Policy Header Not Set	Low	7 (87.5%)
X-Content-Type-Options Header Missing	Low	36 (450.0%)
Storable and Cacheable Content	Informational	38 (475.0%)
User Agent Fuzzer	Informational	22 (275.0%)
Total		8

Alerts

1. Risk=Medium, Confidence=High (2)

1. http://www.itsecgames.com (2)

1. [Content Security Policy \(CSP\) Header Not Set](#) (1)

▼ GET http://www.itsecgames.com

- [CWE-693](#)
- [OWASP_2021_A05](#)
- [OWASP_2017_A06](#)
- POLICY_QA STD =
- POLICY_PENTEST =

Alert tags

Alert 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.

▼ Request line and header section (236 bytes)

```
GET http://www.itsecgames.com HTTP/1.1
host: www.itsecgames.com
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

▼ Request body (0 bytes)

▼ Status line and header section (237 bytes)

```
HTTP/1.1 200 OK
Date: Sat, 27 Sep 2025 14:07:08 GMT
Server: Apache
Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT
ETag: "e43-5d7959bd3c800"
Accept-Ranges: bytes
Content-Length: 3651
Vary: Accept-Encoding
Content-Type: text/html
```

Response

► Response body (3651 bytes)

Solution

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

2. [Sub Resource Integrity Attribute Missing](#) (1)

▼ GET http://www.itsecgames.com

- [CWE-345](#)

Alert tags	<ul style="list-style-type: none"> ▪ OWASP_2021_A05 ▪ OWASP_2017_A06 ▪ POLICY_QA_STD = ▪ POLICY_PENTEST = ▪ POLICY_DEV_STD =
Alert description	The integrity attribute is missing on a script or link tag served by an external server. The integrity tag prevents an attacker who have gained access to this server from injecting a malicious content.
Request	<p>▼ Request line and header section (236 bytes)</p> <pre>GET http://www.itsecgames.com HTTP/1.1 host: www.itsecgames.com 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</pre> <p>▼ Request body (0 bytes)</p> <p>▼ Status line and header section (237 bytes)</p> <pre>HTTP/1.1 200 OK Date: Sat, 27 Sep 2025 14:07:08 GMT Server: Apache Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT ETag: "e43-5d7959bd3c800" Accept-Ranges: bytes Content-Length: 3651 Vary: Accept-Encoding Content-Type: text/html</pre> <p>► Response body (3651 bytes)</p>
Response	
Evidence	<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">
Solution	Provide a valid integrity attribute to the tag.

2. Risk=Medium, Confidence=Medium (1)

1. <http://www.itsecgames.com> (1)

1. [Missing Anti-clickjacking Header](#) (1)

Alert tags	<p>▼ GET http://www.itsecgames.com</p> <ul style="list-style-type: none"> ▪ WSTG-v42-CLNT-09 ▪ OWASP_2021_A05 ▪ OWASP_2017_A06 ▪ POLICY_QA_STD = ▪ POLICY_PENTEST = ▪ CWE-1021
Alert description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Request	<p>▼ Request line and header section (236 bytes)</p> <pre>GET http://www.itsecgames.com HTTP/1.1 host: www.itsecgames.com 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</pre> <p>▼ Request body (0 bytes)</p> <p>▼ Status line and header section (237 bytes)</p> <pre>HTTP/1.1 200 OK Date: Sat, 27 Sep 2025 14:07:08 GMT Server: Apache Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT ETag: "e43-5d7959bd3c800" Accept-Ranges: bytes Content-Length: 3651 Vary: Accept-Encoding Content-Type: text/html</pre> <p>► Response body (3651 bytes)</p>
Response	
Parameter	x-frame-options
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.
Solution	If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

3. Risk=Low, Confidence=Medium (3)

1. <http://www.itsecgames.com> (3)

1. [Insufficient Site Isolation Against Spectre Vulnerability \(1\)](#)

▼ GET http://www.itsecgames.com

- [OWASP 2017 A03](#)
- [OWASP 2021 A04](#)

Alert tags

- [CWE-693](#)
- POLICY_QA STD =
- POLICY_PENTEST =

Alert description Cross-Origin-Resource-Policy header is an opt-in header designed to counter side-channels attacks like Spectre. Resource should be specifically set as shareable amongst different origins.

▼ Request line and header section (236 bytes)

GET http://www.itsecgames.com HTTP/1.1

host: www.itsecgames.com

Request

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 (0 bytes)

▼ Status line and header section (237 bytes)

HTTP/1.1 200 OK

Date: Sat, 27 Sep 2025 14:07:08 GMT

Server: Apache

Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT

Response

Etag: "e43-5d7959bd3c800"

Accept-Ranges: bytes

Content-Length: 3651

Vary: Accept-Encoding

Content-Type: text/html

► Response body (3651 bytes)

Parameter Cross-Origin-Resource-Policy

Ensure that the application/web server sets the Cross-Origin-Resource-Policy header appropriately, and that it sets the Cross-Origin-Resource-Policy header to 'same-origin' for all web pages.

Solution

'same-site' is considered as less secured and should be avoided.

If resources must be shared, set the header to 'cross-origin'.

If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Resource-Policy header (https://caniuse.com/mdn-http_headers_cross-origin-resource-policy).

2. [Permissions Policy Header Not Set \(1\)](#)

▼ GET http://www.itsecgames.com

- [OWASP 2021 A01](#)
- [OWASP 2017 A05](#)

Alert tags

- [CWE-693](#)
- POLICY_QA STD =
- POLICY_PENTEST =

Alert description

Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.

▼ Request line and header section (236 bytes)

GET http://www.itsecgames.com HTTP/1.1

host: www.itsecgames.com

Request

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 (0 bytes)

▼ Status line and header section (237 bytes)

HTTP/1.1 200 OK

Date: Sat, 27 Sep 2025 14:07:08 GMT

Server: Apache

Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT

Response

Etag: "e43-5d7959bd3c800"

Accept-Ranges: bytes

Content-Length: 3651

Vary: Accept-Encoding

Content-Type: text/html

► Response body (3651 bytes)

Solution

Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.

3. [X-Content-Type-Options Header Missing \(1\)](#)

Alert tags	▼ GET http://www.itsecgames.com <ul style="list-style-type: none"> ■ CWE-693 ■ OWASP_2021_A05 ■ OWASP_2017_A06 ■ POLICY_QA_STD = ■ POLICY_PENTEST =
	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.
Other info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Request	▼ Request line and header section (236 bytes) GET http://www.itsecgames.com HTTP/1.1 host: www.itsecgames.com 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 (0 bytes)
Response	▼ Status line and header section (237 bytes) HTTP/1.1 200 OK Date: Sat, 27 Sep 2025 14:07:08 GMT Server: Apache Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT ETag: "e43-5d7959bd3c800" Accept-Ranges: bytes Content-Length: 3651 Vary: Accept-Encoding Content-Type: text/html
	► Response body (3651 bytes)
Parameter	x-content-type-options
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.

4. Risk=Informational, Confidence=Medium (2)

1. http://www.itsecgames.com (2)

1. [Storable and Cacheable Content](#) (1)

Alert tags	▼ GET http://www.itsecgames.com <ul style="list-style-type: none"> ■ WSTG-v42-ATHN-06 ■ POLICY_PENTEST = ■ CWE-524
	The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Other info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
Request	▼ Request line and header section (236 bytes) GET http://www.itsecgames.com HTTP/1.1 host: www.itsecgames.com 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 (0 bytes)
Response	▼ Status line and header section (237 bytes) HTTP/1.1 200 OK Date: Sat, 27 Sep 2025 14:07:08 GMT Server: Apache Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT ETag: "e43-5d7959bd3c800" Accept-Ranges: bytes Content-Length: 3651 Vary: Accept-Encoding

Content-Type: text/html

► Response body (3651 bytes)

Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:

Cache-Control: no-cache, no-store, must-revalidate, private

Solution

Pragma: no-cache

Expires: 0

This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.

2. **User Agent Fuzzer (1)**

▼ GET http://www.itsecgames.com/downloads

Alert tags

- CUSTOM_PAYLOADS =
- POLICY_PENTEST =

Alert

Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler).

description

Compares the response statuscode and the hashcode of the response body with the original response.

▼ Request line and header section (221 bytes)

GET http://www.itsecgames.com/downloads HTTP/1.1
host: www.itsecgames.com
user-agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
pragma: no-cache
cache-control: no-cache
referer: http://www.itsecgames.com

Request

▼ Request body (0 bytes)

▼ Status line and header section (145 bytes)

HTTP/1.1 403 Forbidden
Date: Sat, 27 Sep 2025 14:22:11 GMT
Server: Apache
Content-Length: 199
Content-Type: text/html; charset=iso-8859-1

Response

▼ Response body (199 bytes)

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
</body></html>
```

Parameter

Header User-Agent

Attack

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

Appendix

Alert Types

This section contains additional information on the types of alerts in the report.

1. **Content Security Policy (CSP) Header Not Set**

Source

raised by a passive scanner ([Content Security Policy \(CSP\) Header Not Set](#))

CWE ID

[693](#)

WASC ID

15

Reference

1. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP>
2. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
3. <https://www.w3.org/TR/CSP/>
4. <https://w3c.github.io/webappsec-csp/>
5. <https://web.dev/articles/csp>
6. <https://caniuse.com/#feat=contentsecuritypolicy>
7. <https://content-security-policy.com/>

2. **Missing Anti-clickjacking Header**

Source

raised by a passive scanner ([Anti-clickjacking Header](#))

CWE ID

[1021](#)

WASC ID

15

Reference

1. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options>

3. **Sub Resource Integrity Attribute Missing**

Source raised by a passive scanner ([Sub Resource Integrity Attribute Missing](#))
CWE ID [345](#)
WASC ID 15
Reference 1. https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

4. Insufficient Site Isolation Against Spectre Vulnerability

Source raised by a passive scanner ([Insufficient Site Isolation Against Spectre Vulnerability](#))
CWE ID [693](#)
WASC ID 14
Reference 1. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cross-Origin-Embedder-Policy>

5. Permissions Policy Header Not Set

Source raised by a passive scanner ([Permissions Policy Header Not Set](#))
CWE ID [693](#)
WASC ID 15
1. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Permissions-Policy>
2. <https://developer.chrome.com/blog/feature-policy/>
Reference 3. <https://scotthelme.co.uk/a-new-security-header-feature-policy/>
4. <https://w3c.github.io/webappsec-feature-policy/>
5. <https://www.smashingmagazine.com/2018/12/feature-policy/>

6. X-Content-Type-Options Header Missing

Source raised by a passive scanner ([X-Content-Type-Options Header Missing](#))
CWE ID [693](#)
WASC ID 15
Reference 1. [https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941\(v=vs.85\)](https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85))
2. <https://owasp.org/www-community/Security-Headers>

7. Storable and Cacheable Content

Source raised by a passive scanner ([Content Cacheability](#))
CWE ID [524](#)
WASC ID 13
Reference 1. <https://datatracker.ietf.org/doc/html/rfc7234>
2. <https://datatracker.ietf.org/doc/html/rfc7231>
3. <https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html>

8. User Agent Fuzzer

Source raised by an active scanner ([plugin ID: 10104](#))
Reference 1. <https://owasp.org/wstg>