

# Security Scan Report

Target: <https://google.com>

Scan Type: FULL

Generated: Mon Dec 15 22:20:49 IST 2025

## Executive Summary

High: 0

Medium: 0

Low: 2

Informational: 2

## Detailed Findings

### ZAP is Out of Date

#### Affected URLs:

<https://google.com>

#### Description:

The version of ZAP you are using to test your app is out of date and is no longer being updated.

The risk level is set based on how out of date your ZAP version is.

#### Recommended Fix:

Download the latest version of ZAP from <https://www.zaproxy.org/download/> and install it.

---

#### Affected URLs:

<https://google.com>

#### Description:

The version of ZAP you are using to test your app is out of date and is no longer being updated.

The risk level is set based on how out of date your ZAP version is.

**Recommended Fix:**

Download the latest version of ZAP from <https://www.zaproxy.org/download/> and install it.

---

## Strict-Transport-Security Header Not Set

**Affected URLs:**

<https://google.com>  
<https://google.com/sitemap.xml>  
<https://google.com/robots.txt>

**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.

**Recommended Fix:**

Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

---

**Affected URLs:**

<https://google.com>  
<https://google.com/sitemap.xml>  
<https://google.com/robots.txt>

**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.

**Recommended Fix:**

Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

---

# User Agent Fuzzer

### Affected URLs:

[illegible]

**Description:**

Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

**Recommended Fix:**

---

**Affected URLs:**

https://google.com/robots.txt  
https://google.com/sitemap.xml  
https://google.com/robots.txt  
https://google.com/sitemap.xml  
https://google.com/robots.txt  
https://google.com/sitemap.xml  
https://google.com/robots.txt  
https://google.com  
https://google.com/robots.txt  
https://google.com/sitemap.xml  
https://google.com/robots.txt  
https://google.com/sitemap.xml  
https://google.com/sitemap.xml  
https://google.com  
https://google.com/robots.txt  
https://google.com/sitemap.xml  
https://google.com/robots.txt  
https://google.com/sitemap.xml  
https://google.com/sitemap.xml  
https://google.com/robots.txt  
https://google.com/sitemap.xml  
https://google.com/robots.txt  
https://google.com/sitemap.xml  
https://google.com/robots.txt  
https://google.com/sitemap.xml  
https://google.com  
https://google.com/robots.txt  
https://google.com  
https://google.com  
https://google.com  
https://google.com

https://google.com  
https://google.com  
https://google.com  
https://google.com

**Description:**

Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

**Recommended Fix:**

---

## Retrieved from Cache

**Affected URLs:**

https://google.com/sitemap.xml  
https://google.com/robots.txt

**Description:**

The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

**Recommended Fix:**

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

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.

---

**Affected URLs:**

<https://google.com/sitemap.xml>

<https://google.com/robots.txt>

**Description:**

The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network.

This configuration is typically found in corporate or educational environments, for instance.

**Recommended Fix:**

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

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.

---