# SecuFusion Scan Report

Scan Date: 24/03/2025, 12:46:11

## Scan Summary

**Total Issues: 48**

**True Positives: 42**

**False Positives: 6**

## Table of Contents



## 1. True Positives

### Vulnerability 1: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 2: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 3: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 4: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 5: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 6: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 7: Content Security Policy (CSP) Header Not Set

**Risk:** Medium

**OWASP Category:**

**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.

**Solution:**

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

## Vulnerability 8: Content Security Policy (CSP) Header Not Set

**Risk:** Medium

**OWASP Category:**

**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.

**Solution:**

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

## Vulnerability 9: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 10: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 11: Cross-Domain JavaScript Source File Inclusion

**Risk:** Low

**OWASP Category:**

**Description:**

The page includes one or more script files from a third-party domain.

**Solution:**

Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

## Vulnerability 12: Cross-Domain JavaScript Source File Inclusion

**Risk:** Low

**OWASP Category:**

**Description:**

The page includes one or more script files from a third-party domain.

**Solution:**

Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

## Vulnerability 13: Cross-Domain JavaScript Source File Inclusion

**Risk:** Low

**OWASP Category:**

**Description:**

The page includes one or more script files from a third-party domain.

**Solution:**

Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

## Vulnerability 14: Cross-Domain JavaScript Source File Inclusion

**Risk:** Low

**OWASP Category:**

**Description:**

The page includes one or more script files from a third-party domain.

**Solution:**

Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

## Vulnerability 15: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 16: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 17: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 18: Content Security Policy (CSP) Header Not Set

**Risk:** Medium

**OWASP Category:**

**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.

**Solution:**

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

## Vulnerability 19: Content Security Policy (CSP) Header Not Set

**Risk:** Medium

**OWASP Category:**

**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.

**Solution:**

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

## Vulnerability 20: Content Security Policy (CSP) Header Not Set

**Risk:** Medium

**OWASP Category:**

**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.

**Solution:**

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

## Vulnerability 21: Content Security Policy (CSP) Header Not Set

**Risk:** Medium

**OWASP Category:**

**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.

**Solution:**

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

## Vulnerability 22: Content Security Policy (CSP) Header Not Set

**Risk:** Medium

**OWASP Category:**

**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.

**Solution:**

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

## Vulnerability 23: Content Security Policy (CSP) Header Not Set

**Risk:** Medium

**OWASP Category:**

**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.

**Solution:**

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

## Vulnerability 24: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 25: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 26: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 27: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 28: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 29: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 30: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 31: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 32: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 33: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 34: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 35: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 36: Content Security Policy (CSP) Header Not Set

**Risk:** Medium

**OWASP Category:**

**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.

**Solution:**

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

## Vulnerability 37: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 38: Content Security Policy (CSP) Header Not Set

**Risk:** Medium

**OWASP Category:**

**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.

**Solution:**

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

## Vulnerability 39: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 40: Content Security Policy (CSP) Header Not Set

**Risk:** Medium

**OWASP Category:**

**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.

**Solution:**

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

## Vulnerability 41: Cross-Domain Misconfiguration

**Risk:** Medium

**OWASP Category:** A05:2021 - Security Misconfiguration

**Description:**

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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.

## Vulnerability 42: Cloud Metadata Potentially Exposed

**Risk:** High

**OWASP Category:**

**Description:**

The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure.
All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Host header field.

**Solution:**

Do not trust any user data in NGINX configs. In this case it is probably the use of the $host variable which is set from the 'Host' header and can be controlled by an attacker.

# 2. False Positives

## Vulnerability 1: Modern Web Application

**Risk:** Informational

**OWASP Category:**

**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.

**Solution:**

This is an informational alert and so no changes are required.

## Vulnerability 2: Modern Web Application

**Risk:** Informational

**OWASP Category:**

**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.

**Solution:**

This is an informational alert and so no changes are required.

## Vulnerability 3: Information Disclosure - Suspicious Comments

**Risk:** Informational

**OWASP Category:**

**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.

**Solution:**

Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

## Vulnerability 4: Timestamp Disclosure - Unix

**Risk:** Low

**OWASP Category:**

**Description:**

A timestamp was disclosed by the application/web server. - Unix

**Solution:**

Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

## Vulnerability 5: Information Disclosure - Suspicious Comments

**Risk:** Informational

**OWASP Category:**

**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.

**Solution:**

Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

## Vulnerability 6: Modern Web Application

**Risk:** Informational

**OWASP Category:**

**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.

**Solution:**

This is an informational alert and so no changes are required.