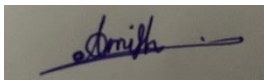
Sri Lanka Institute of Information Technology

Audit Report

IE3042-Secure Software System

Year 3, Semester 2

IT NUMBER	NAME	CONTACT NUMBER	EMAIL	Signature
IT21167478	Nilupul S.A	0769665153	It21167478@my.sliit.lk	
IT21167096	De Zoysa A. S.	0719895280	it21167096@my.sliit.lk	

Company Name	:	Serendib Sentinel Technology
Location	:	Cinnamon Life, 800 Sir James Peiris Mawatha, Colombo 02, Sri Lanka
Subject of Audit	:	Secure Chat Application
Audit Date	:	14.05.2024.
Auditor	:	Amith Nilupul Senevirathne
		Sayonara De Zoysa
Signature	:	
		

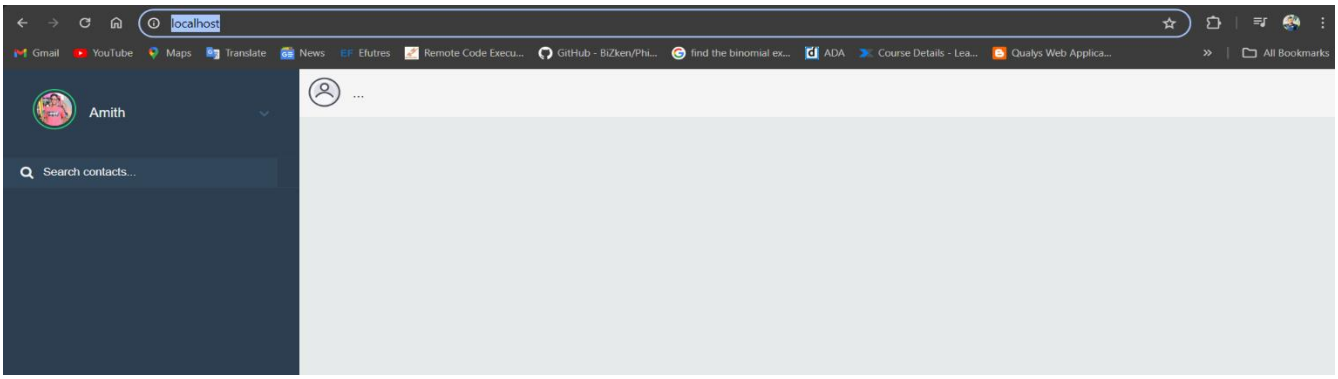
Disclaimer

This audit report for Serendib Sentinel Technology's secure chat application, located at Cinnamon Life, 800 Sir James Peiris Mawatha, Colombo 02, Sri Lanka, dated May 14, 2024, is for the company's and its stakeholders' only personal use and information. The conclusions and suggestions presented in this report are based on the information supplied and the conditions observed during the audit period. Serendib Sentinel Technology and the audit team accept no responsibility for any actions made by third parties based on this report. The report cannot guarantee total security or the absence of vulnerabilities since security situations and threat environments are always changing. Because cybersecurity risks and attacks evolve at such a rapid pace, no organizational asset can be guaranteed complete security. This report contains no guarantees or certifications provided by the audit team. The audit team will never be held accountable for indirect occurrences, whether or not they were made aware of the possibility.

Table of Contents

Executive Summary

Following the audit, the following vulnerabilities in the Secure chat application was uncovered.



Site: http://localhost

Generated on Sun, 19 May 2024 19:03:24

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	6
Low	2
Informational	6

Alerts

Name	Risk Level	Number of Instances
CSP: Wildcard Directive	Medium	2
Content Security Policy (CSP) Header Not Set	Medium	2
Cross-Domain Misconfiguration	Medium	8
Missing Anti-clickjacking Header	Medium	2
Session ID in URL Rewrite	Medium	8
Vulnerable JS Library	Medium	1
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	18
X-Content-Type-Options Header Missing	Low	24
Cookie Poisoning	Informational	5
Information Disclosure - Suspicious Comments	Informational	12
Loosely Scoped Cookie	Informational	8
Modern Web Application	Informational	2
Session Management Response Identified	Informational	14
User Agent Fuzzer	Informational	96

General Information

Serendib Sentinel Technology is a leading technology company based at Cinnamon Life, 800 Sir James Peiris Mawatha, Colombo 02, Sri Lanka. Under the expert guidance of the management team, including key personnel Kasun Karunarathna and Mafaz Farahid the organization has grown to become a prominent player in the field of secure communication solutions.

On May 14, 2024, a comprehensive audit was conducted on Serendib Sentinel Technology's secure chat application. This audit aimed to evaluate the application's security features, ensuring they meet the highest standards of data protection and privacy. The secure chat application is designed to provide encrypted communication for users, safeguarding sensitive information against unauthorized access and cyber threats.

The audit's scope included a thorough review of the application's architecture, encryption protocols, and user authentication mechanisms. The findings and recommendations will help Serendib Sentinel Technology enhance the security and reliability of its chat application, reinforcing its commitment to delivering robust and secure communication solutions.

Purpose

This audit was conducted for the below objectives.

- *Security Assessment:* Evaluating a secure chat application's security posture is the main goal of an audit. This includes looking at the application's implementation overall, authentication procedures, encryption techniques, and architectural design to find any flaws or vulnerabilities that an attacker may exploit.

- *Compliance Verification:* Secure communication is required by law in many sectors, particularly those that deal with sensitive data like healthcare and banking. Auditing aids in confirming that the chat program conforms with pertinent laws including PCI DSS, GDPR, and HIPAA.

- *Risk Mitigation:* Auditing assists in reducing the possibility of data breaches, illegal access, or other security incidents that might jeopardize the availability, confidentiality, or integrity of sensitive information shared via the chat program. Auditing does this by locating and fixing security vulnerabilities.

- *Quality Assurance:* Auditing contributes to the chat application's overall quality as well. Auditors can offer input on areas to improve performance, usability, and reliability by assessing its design, coding, and implementation.

- *Believe and Confidence*: Users and stakeholders are more likely to believe and have faith in a secure chat application's security capability when they are aware that it has undergone extensive audits. Businesses and organizations who depend on secure communication for delicate or private affairs may find this to be especially crucial.

- *Continuous Improvement:* Rather than being a one-time occurrence, auditing need to be a continuous practice. Frequent audits contribute to the chat application's continued compliance and security as threats change and technology improves. Additionally, they offer chances for ongoing development predicated on input and insights gained from earlier audits.

Internal support Team

Name
Kasun Karunarathne
Mafaz Farhad
Mishen Johan Wellalage
Sakkya Jayawardane
Melanie Jayasundara
Shashini Navodaya Ranathunga

Identified Vulnerabilities

CSP: Wildcard Directive

Medium	CSP: Wildcard Directive
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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	http://localhost/robots.txt
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://localhost/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Content Security Policy (CSP) Header Not Set

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	http://localhost
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost/
Method	GET
Attack	
Evidence	
Other Info	
Instances	2

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/Security/CSP/Introducing_Content_Security_Policy 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

Cross-Domain Misconfiguration

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	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyWGq
Method	GET
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	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXCh&sid=kzdhXwRX2WaidlckAAAE
Method	GET
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	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXpY
Method	GET
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	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXrR&sid=Ap1HAD7-Sf-3sk8-AAAF
Method	GET
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	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXxF&sid=Ap1HAD7-Sf-3sk8-AAAF
Method	GET
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	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
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	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZqH&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
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	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZqH&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
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	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
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	8
	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

Solution	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?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Missing Anti-clickjacking Header

Medium	Missing Anti-clickjacking Header
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	http://localhost
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost/
Method	GET
Attack	
Evidence	
Other Info	
Instances	2
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. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Session ID in URL Rewrite

Medium	Session ID in URL Rewrite
Description	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXCh&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	
Evidence	kzdhXwRX2WaidlckAAAE
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXrR&sid=Ap1HAD7-Sf-3sk8-AAAF
Method	GET
Attack	
Evidence	Ap1HAD7-Sf-3sk8-AAAF
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXxF&sid=Ap1HAD7-Sf-3sk8-AAAF
Method	GET
Attack	
Evidence	Ap1HAD7-Sf-3sk8-AAAF
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZqH&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	
Evidence	qa_qX-hp7SiUjL1eAAAG
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	
Evidence	qa_qX-hp7SiUjL1eAAAG
Other Info	

URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	
Evidence	kzdhXwRX2WaidlckAAAE
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	
Evidence	qa_qX-hp7SiUjL1eAAAG
Other Info	
Instances	8

Solution	For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Reference	https://seclists.org/webappsec/2002/q4/111
CWE Id	200
WASC Id	13
Plugin Id	3

Vulnerable JS Library

Medium	Vulnerable JS Library
Description	The identified library jquery, version 3.3.1 is vulnerable.
URL	http://localhost/js/jquery-3.3.1.min.js
Method	GET
Attack	
Evidence	jquery-3.3.1.min.js
Other Info	CVE-2020-11023 CVE-2020-11022 CVE-2019-11358
Instances	1
Solution	Please upgrade to the latest version of jquery.
Reference	https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
CWE Id	829
WASC Id	
Plugin Id	10003

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Low	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	http://localhost
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/css/font-awesome.min.css
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other	

Info	
URL	http://localhost/css/login.css
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/css/reset.min.css
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/css/stylesheet.css
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/fonts/fontawesome-webfont.woff2?v=4.7.0
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/img/favicon.ico
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/img/unnamed.gif
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/img/unnamed.png
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/js/client.js

Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/js/crypto-js/crypto-js.js
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/js/crypto.js
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/js/jquery-3.3.1.min.js
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/js/jsencrypt.min.js
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/js/socket.io.js
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/robots.txt
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost/sitemap.xml
Method	GET

Attack	
Evidence	X-Powered-By: Express
Other Info	
Instances	18
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037

X-Content-Type-Options Header Missing

Low	X-Content-Type-Options Header Missing
Description	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.
URL	http://localhost
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/css/font-awesome.min.css
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/css/login.css
Method	GET
Attack	
Evidence	

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.
URL	http://localhost/css/reset.min.css
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/css/stylesheet.css
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/fonts/fontawesome-webfont.woff2?v=4.7.0
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/img/favicon.ico
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/img/unnamed.gif
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/img/unnamed.png
Method	GET
Attack	
Evidence	

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.
URL	http://localhost/js/client.js
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/js/crypto-js/crypto-js.js
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/js/crypto.js
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/js/jquery-3.3.1.min.js
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/js/jsencrypt.min.js
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/js/socket.io.js
Method	GET
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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.
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyWGq
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXCh&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXpY
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXrR&sid=Ap1HAD7-Sf-3sk8-AAAF
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXxF&sid=Ap1HAD7-Sf-3sk8-AAAF
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	
Evidence	

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.
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZqH&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	
Evidence	
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.
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	
Evidence	
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.
Instances	24
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.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Cookie Poisoning

Informational	Cookie Poisoning
Description	This check looks at user-supplied input in query string parameters and POST data to identify where cookie parameters might be controlled. This is called a cookie poisoning attack, and becomes exploitable when an attacker can manipulate the cookie in various ways. In some cases this will not be exploitable, however, allowing URL parameters to set cookie values is generally considered a bug.
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXCh&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXCh&sid=kzdhXwRX2WaidlckAAAE User-input was found in the following cookie: io=kzdhXwRX2WaidlckAAAE; Path=/; HttpOnly; SameSite=Strict The user input was: sid=kzdhXwRX2WaidlckAAAE

URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXrR&sid=Ap1HAD7-Sf-3sk8-AAAF
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXrR&sid=Ap1HAD7-Sf-3sk8-AAAF User-input was found in the following cookie: io=Ap1HAD7-Sf-3sk8-AAAF; Path=/; HttpOnly; SameSite=Strict The user input was: sid=Ap1HAD7-Sf-3sk8-AAAF
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXxF&sid=Ap1HAD7-Sf-3sk8-AAAF
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXxF&sid=Ap1HAD7-Sf-3sk8-AAAF User-input was found in the following cookie: io=Ap1HAD7-Sf-3sk8-AAAF; Path=/; HttpOnly; SameSite=Strict The user input was: sid=Ap1HAD7-Sf-3sk8-AAAF
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZqH&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZqH&sid=qa_qX-hp7SiUjL1eAAAG User-input was found in the following cookie: io=qa_qX-hp7SiUjL1eAAAG; Path=/; HttpOnly; SameSite=Strict The user input was: sid=qa_qX-hp7SiUjL1eAAAG
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG User-input was found in the following cookie: io=qa_qX-hp7SiUjL1eAAAG; Path=/; HttpOnly; SameSite=Strict The user input was: sid=qa_qX-hp7SiUjL1eAAAG
Instances	5
Solution	Do not allow user input to control cookie names and values. If some query string parameters must be set in cookie values, be sure to filter out semicolon's that can serve as name/value pair delimiters.
Reference	https://en.wikipedia.org/wiki/HTTP_cookie https://cwe.mitre.org/data/definitions/565.html
CWE Id	565
WASC Id	20
Plugin Id	10029

Information Disclosure-Suspicious Comments

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	http://localhost/js/client.js
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 7 times, the first in the element starting with: "// when a client socket disconnected or a channel admin be offline", see evidence field for the suspicious comment/snippet.
URL	http://localhost/js/client.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 14 times, the first in the element starting with: "// when me sign-in was expired from server time", see evidence field for the suspicious comment/snippet.
URL	http://localhost/js/client.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " alert("Please first select a chat to sending message!");", see evidence field for the suspicious comment/snippet.
URL	http://localhost/js/client.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 19 times, the first in the element starting with: "// save the my user data when I signed-in to server successfully", see evidence field for the suspicious comment/snippet.
URL	http://localhost/js/client.js
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 8 times, the first in the element starting with: " $("#yourName").val(me.username);", see evidence field for the suspicious comment/snippet.
URL	http://localhost/js/crypto-js/crypto-js.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 15 times, the first in the element starting with: " * Creates a new object that inherits from this object.", see evidence field for the suspicious comment/snippet.
URL	http://localhost/js/crypto-js/crypto-js.js

Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 5 times, the first in the element starting with: " // Masks that select the SBOX input", see evidence field for the suspicious comment/snippet.
URL	http://localhost/js/crypto-js/crypto-js.js
Method	GET
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 2 times, the first in the element starting with: " * @param {number} offset The offset where the block starts.", see evidence field for the suspicious comment/snippet.
URL	http://localhost/js/crypto.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "// define the characters to pick from", see evidence field for the suspicious comment /snippet.
URL	http://localhost/js/jquery-3.3.1.min.js
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports? module.exports=e.document?t(e,!0):function(", see evidence field for the suspicious comment/snippet.
URL	http://localhost/js/jsencrypt.min.js
Method	GET
Attack	
Evidence	DB
Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "! function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports):"function" ==typeof define&&define.amd?define(["ex", see evidence field for the suspicious comment /snippet.
URL	http://localhost/js/socket.io.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 2 times, the first in the element starting with: " return function (t) { function e(r) { if (n[r]) return n[r].exports; var o = n [r] = { exports: {}, id: r, loaded: !1 }; retu", see evidence field for the suspicious comment /snippet.
Instances	12
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	

Loosely Scoped Cookie

Informational	Loosely Scoped Cookie
Description	Cookies can be scoped by domain or path. This check is only concerned with domain scope. The domain scope applied to a cookie determines which domains can access it. For example, a cookie can be scoped strictly to a subdomain e.g. www.nottrusted.com, or loosely scoped to a parent domain e.g. nottrusted.com. In the latter case, any subdomain of nottrusted.com can access the cookie. Loosely scoped cookies are common in mega-applications like google.com and live.com. Cookies set from a subdomain like app.foo.bar are transmitted only to that domain by the browser. However, cookies scoped to a parent-level domain may be transmitted to the parent, or any subdomain of the parent.
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyWGq
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost io=kzdhXwRX2WaidlckAAAE
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXCh&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost io=kzdhXwRX2WaidlckAAAE
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXpY
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost io=Ap1HAD7-Sf-3sk8-AAAF
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXrR&sid=Ap1HAD7-Sf-3sk8-AAAF
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost io=Ap1HAD7-Sf-3sk8-AAAF
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXxF&sid=Ap1HAD7-Sf-3sk8-AAAF
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost io=Ap1HAD7-Sf-3sk8-AAAF
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET

Attack Evidence	
Other Info	The origin domain used for comparison was: localhost io=qa_qX-hp7SiUjL1eAAAG
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZqH&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack Evidence Other Info	The origin domain used for comparison was: localhost io=qa_qX-hp7SiUjL1eAAAG
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack Evidence	
Other Info	The origin domain used for comparison was: localhost io=qa_qX-hp7SiUjL1eAAAG
Instances	8
Solution	Always scope cookies to a FQDN (Fully Qualified Domain Name).
Reference	https://tools.ietf.org/html/rfc6265#section-4.1 https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies
CWE Id	565
WASC Id	15
Plugin Id	90033

Modern Web Application

Informational	Modern Web Application
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.
URL	http://localhost
Method	GET
Attack	
Evidence	<script type="text/javascript" src="js/jquery-3.3.1.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost/
Method	GET
Attack	
Evidence	<script type="text/javascript" src="js/jquery-3.3.1.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	2
Solution	This is an informational alert and so no changes are required.
Reference	

CWE Id	
WASC Id	
Plugin Id	10109

Session Management Response Identified

Informational	Session Management Response Identified
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyWGq
Method	GET
Attack	
Evidence	kzdhXwRX2WaidlckAAAE
Other Info	cookie:io
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXCh&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	
Evidence	kzdhXwRX2WaidlckAAAE
Other Info	cookie:io
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXpY
Method	GET
Attack	
Evidence	Ap1HAD7-Sf-3sk8-AAAF
Other Info	cookie:io
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXrR&sid=Ap1HAD7-Sf-3sk8-AAAF
Method	GET
Attack	
Evidence	Ap1HAD7-Sf-3sk8-AAAF
Other Info	cookie:io
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXxF&sid=Ap1HAD7-Sf-3sk8-AAAF
Method	GET
Attack	
Evidence	Ap1HAD7-Sf-3sk8-AAAF
Other Info	cookie:io
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	
Evidence	qa_qX-hp7SiUjL1eAAAG

Other Info	cookie:io
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZqH&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	
Evidence	qa_qX-hp7SiUjL1eAAAG
Other Info	cookie:io
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	
Evidence	qa_qX-hp7SiUjL1eAAAG
Other Info	cookie:io
URL	http://localhost/css/reset.min.css
Method	GET
Attack	
Evidence	kzdhXwRX2WaidlckAAAE
Other Info	cookie:io
URL	http://localhost/fonts
Method	GET
Attack	
Evidence	Ap1HAD7-Sf-3sk8-AAAF
Other Info	cookie:io
URL	http://localhost/img/unnamed.png
Method	GET
Attack	
Evidence	Ap1HAD7-Sf-3sk8-AAAF
Other Info	cookie:io
URL	http://localhost/img/unnamed.png
Method	GET
Attack	
Evidence	kzdhXwRX2WaidlckAAAE
Other Info	cookie:io
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyXxF&sid=Ap1HAD7-Sf-3sk8-AAAF
Method	GET
Attack	
Evidence	Ap1HAD7-Sf-3sk8-AAAF

Other Info	cookie:io
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	
Evidence	qa_qX-hp7SiUjL1eAAAG
Other Info	cookie:io
Instances	14
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112

User Agent Fuzzer

Informational	User Agent Fuzzer
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.
URL	http://localhost/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost/css
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost/css
Method	GET

Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost/css
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost/css
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost/css
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost/css
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost/css
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost/css
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost/css

Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost/fonts
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost/fonts
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost/fonts
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost/fonts
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost/fonts
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost/fonts
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost/fonts
Method	GET

Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost/fonts
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost/fonts
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost/fonts
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost/fonts
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost/fonts
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost/img
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost/img
Method	GET

Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost/img
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost/img
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost/img
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost/img
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost/img
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost/img
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost/img
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)

Evidence	
Other Info	
URL	http://localhost/img
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost/img
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost/img
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost/js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost/js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost/js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost/js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko

Evidence	
Other Info	
URL	http://localhost/js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost/js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost/js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost/js
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost/js
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost/js
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost/js
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16

Evidence	
Other Info	
URL	http://localhost/js
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost/js/crypto-js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost/js/crypto-js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost/js/crypto-js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost/js/crypto-js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost/js/crypto-js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost/js/crypto-js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Evidence	
Other Info	
URL	http://localhost/js/crypto-js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost/js/crypto-js
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost/js/crypto-js
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost/js/crypto-js
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost/js/crypto-js
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost/js/crypto-js
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	

Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	

Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZp6
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-

URL	hp7SiUjL1eAAAG
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=polling&t=O-GyZxr&sid=qa_qX-hp7SiUjL1eAAAG
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	

URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other	

Info	
URL	http://localhost/socket.io/?EIO=3&transport=websocket&sid=kzdhXwRX2WaidlckAAAE
Method	GET
Attack Evidence Other Info	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Instances Solution	96
Reference CWE Id	https://owasp.org/wstg
WASC Id Plugin Id	10104