



March 22, 2024

39 Everett Drive  
Princeton Junction, NJ 08550  
United States

## Security Update and Future Plans

Entourage owns and supports the software licensed to Edge Photography called CreatorStudio Pro. We have a dedicated application in Canada for Edge to use, built on top of Canadian AWS Cloud Services to comply with Canadian data residency requirements while also providing access to our yearbook software.

Third-party cyber-security experts been engaged and have completed a full forensic review of the CreatorStudio PRO application in Canada. We have conducted an extensive forensic audit of all applications, network and processes and have confirmed the system to be fully operational with added hardened security standards in place. We have engaged two external security firms to conduct continued forensic analysis of all our technology resources and we have undergone six (6) security assessments (listed below) by third party cyber penetration services to confirm that CreatorStudio Pro is secure for continued use by schools in Canada.

The following are highlights from our forensic reports conducted by external cyber-security experts:

- We have confirmed the exact method of attack from the February 2024 data attack incident. As outlined in the *Incident Summary from our Third-Party Security agency*, the attackers illegally accessed a configuration file from one of our development servers. The attackers then used information from the configuration file, specifically AWS Access Keys, to conduct the attack.
- The third-party cyber-security firms have confirmed the exact attack method, steps for remediation, and have collaborated with our team so that we can prevent further attacks on these configuration files.
- The third-party cyber-security firms have conducted a full cyber-security forensic audit of CreatorStudio PRO. Our teams in collaboration with the external cyber-security experts have implemented all recommended changes identified from the forensic audit.
- We have conducted the following application scans of the CreatorStudio PRO application in Canada.
  - HostedScan Security Vulnerability Scan - CVSS Score 2.6 - Low Threat Risk
  - Qualys SSL Labs Security Report - All A reports
  - Securi Website & Malware Scan - Low Security Risk Assessment
  - OWASP ZAP Scan Report
  - PentestTool Website Vulnerability Scan
  - Nmap Scan Report



- The third-party cyber-security firms have reviewed all network and access logs from the attack on our systems. They have confirmed that there has been no other unauthorized access both during and after the attack.
- The third-party cyber-security firms have reviewed email, VPN and GSuite logs also confirms that there was no other unauthorized access via these technology avenues.
- Our team at CreatorStudio PRO have notified both the US and Canadian authorities and we are communicating the details from the attack to help with the ongoing investigation.

Going forward, the CreatorStudio PRO team is committed to enhancing and ensuring the highest security application through the following:

- We have engaged third-party security agencies to conduct ongoing forensic reviews, pro-active access monitoring, and annual penetration tests to continue to improve our security practices. This is part of ongoing security enhancements to ensure continued security improvement.
- We have engaged a third-party dark web monitoring service (TransUnion) to continue to monitor any affected data from the February attack. We will continue to engage in monitoring for a minimum of 90 days.
- We have installed new intrusion detection automation to monitor and remediate against future intrusion attacks. Estimated completion in 30 days.
- We will continue to monitor the database and system to monitor for further evidence of breach or attack.
- We are building offsite backups of all photos by the end of April. We are in the process of adding backups of all photos in S3 buckets resident in Canada.
- We have expanded the use of location-based access restrictions (IP-based restrictions) in all our computing resources to further tighten network security.
- Our staff will undergo annual training on all aspects of cyber security and privacy to ensure continued strict adherence to our policies.

We have provided copies of the application scans and penetration tests referenced above at the end of this letter.

We at CreatorStudio PRO continue to review and monitor our security practices and are committed to providing the most secure yearbook design experience possible. For further questions or clarifications, please contact the technical lead for CreatorStudio PRO, Elias at [elias@creatorstudio.com](mailto:elias@creatorstudio.com).

February 28, 2024

# Vulnerability Scan Report

prepared by

**HostedScan Security**



[hostedscan.com](https://hostedscan.com)

# Overview

---

<b>1</b>	<b>Executive Summary</b>	<b>3</b>
<b>2</b>	<b>Risks By Target</b>	<b>4</b>
<b>3</b>	<b>Network Vulnerabilities</b>	<b>6</b>
<b>4</b>	<b>Glossary</b>	<b>8</b>

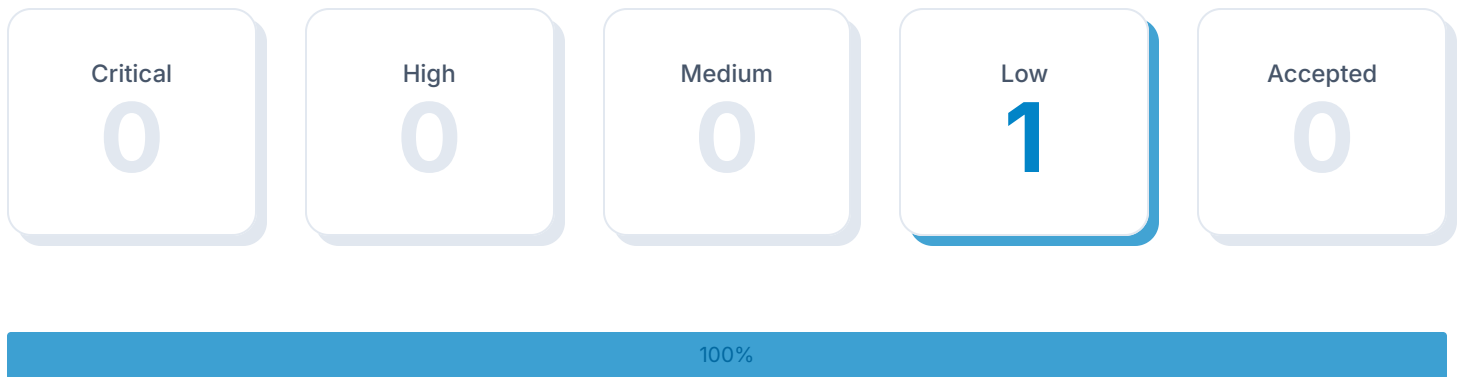


# 1 Executive Summary

Vulnerability scans were conducted on selected servers, networks, websites, and applications. This report contains the discovered potential risks from these scans. Risks have been classified into categories according to the level of threat and degree of potential harm they may pose.

## 1.1 Total Risks

Below is the total number of risks found by severity. High risks are the most severe and should be evaluated first. An accepted risk is one which has been manually reviewed and classified as acceptable to not fix at this time, such as a false positive or an intentional part of the system's architecture.



## 1.2 Report Coverage

This report includes findings for **1 target** that were scanned. Each target is a single URL, IP address, or fully qualified domain name (FQDN).

### Vulnerability Categories

1







Network Vulnerabilities

## 2 Risks By Target

This section contains the vulnerability findings for each target that was scanned. Prioritize the most vulnerable assets first.

### 2.1 Targets Summary

The total number of risks found for each target, by severity.

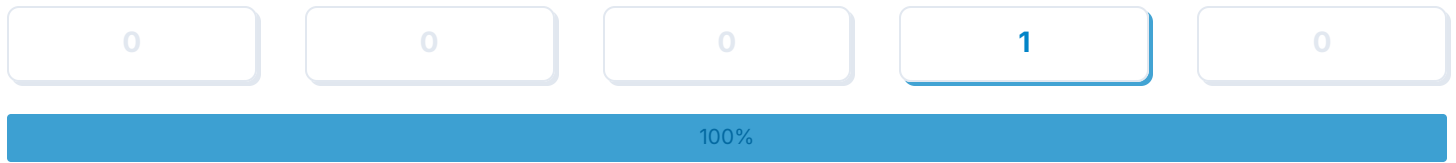
Target	 Critical	 High	 Medium	 Low	 Accepted
 edge.creatorstudiopro.com	0	0	0	1	0

## 2.2 Target Breakdowns

The risks discovered for each target.

 Target  
[edge.creatorstudiopro.com](https://edge.creatorstudiopro.com)

### Total Risks



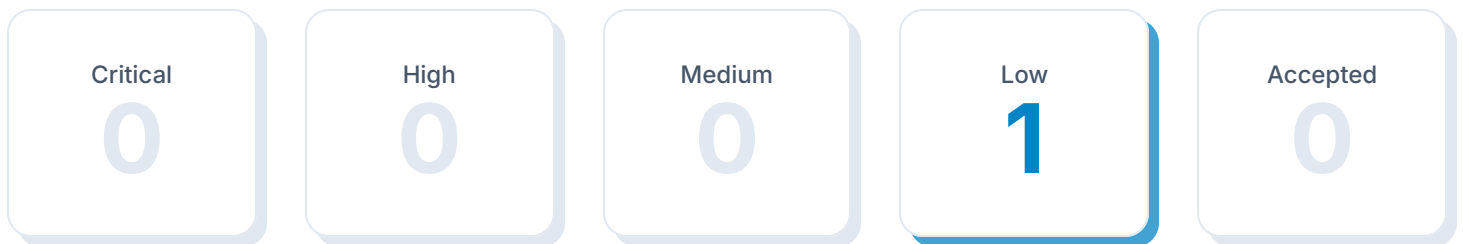
Network Vulnerabilities	Threat Level	First Detected	Last Detected
<a href="#">TCP Timestamps Information Disclosure</a> cvss score: 2.6	<span style="color: blue;">●</span> Low	0 days ago	0 days ago

## 3 Network Vulnerabilities

The OpenVAS network vulnerability scan tests servers and internet connected devices for over 50,000 vulnerabilities. OpenVAS uses the Common Vulnerability Scoring System (CVSS) to quantify the severity of findings. 0.0 is the lowest severity and 10.0 is the highest.

### 3.1 Total Risks

Total number of risks found by severity.



### 3.2 Risks Breakdown

Summary list of all detected risks.

Title	Threat Level	CVSS Score	Open	Accepted
TCP Timestamps Information Disclosure	● Low	2.6	1	0



### 3.3 Full Risk Details

Detailed information about each risk found by the scan.

#### TCP Timestamps Information Disclosure

● Low  
cvss score: 2.6

#### Description

The remote host implements TCP timestamps and therefore allows to compute the uptime.

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

#### Solution

To disable TCP timestamps on linux add the line 'net.ipv4.tcp\_timestamps

#### References

<https://datatracker.ietf.org/doc/html/rfc1323>

<https://datatracker.ietf.org/doc/html/rfc7323>

<https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152>

<https://www.fortiguard.com/psirt/FG-IR-16-090>

Vulnerable Target	First Detected	Last Detected
<a href="https://edge.creatorstudiopro.com">edge.creatorstudiopro.com</a>	0 days ago	0 days ago

## 4 Glossary

### Accepted Risk

An accepted risk is one which has been manually reviewed and classified as acceptable to not fix at this time, such as a false positive or an intentional part of the system's architecture.

### Fully Qualified Domain Name (FQDN)

A fully qualified domain name is a complete domain name for a specific website or service on the internet. This includes not only the website or service name, but also the top-level domain name, such as .com, .org, .net, etc. For example, 'www.example.com' is an FQDN.

### Network Vulnerabilities

The OpenVAS network vulnerability scan tests servers and internet connected devices for over 50,000 vulnerabilities. OpenVAS uses the Common Vulnerability Scoring System (CVSS) to quantify the severity of findings. 0.0 is the lowest severity and 10.0 is the highest.

### Risk

A risk is a finding from a vulnerability scan. Each risk is a potential security issue that needs review. Risks are assigned a threat level which represents the potential severity.

### Target

A target represents target is a single URL, IP address, or fully qualified domain name (FQDN) that was scanned.

### Threat Level

The threat level represents the estimated potential severity of a particular risk. Threat level is divided into 4 categories: High, Medium, Low and Accepted.

### Threat Level

The threat level represents the estimated potential severity of a particular risk. Threat level is divided into 5 categories: Critical, High, Medium, Low and Accepted.

### CVSS Score

The CVSS 3.0 score is a global standard for evaluating vulnerabilities with a 0 to 10 scale. CVSS maps to threat levels: 0.1 - 3.9 = Low, 4.0 - 6.9 = Medium, 7.0 - 8.9 = High, 9.0 - 10.0 = Critical

This report was prepared using

## HostedScan Security®

For more information, visit [hostedscan.com](https://hostedscan.com)

Founded in Seattle, Washington in 2019, HostedScan, LLC. is dedicated to making continuous vulnerability scanning and risk management much more easily accessible to more businesses.



HostedScan, LLC.

2212 Queen Anne Ave N  
Suite #521  
Seattle, WA 98109

Terms & Policies  
[hello@hostedscan.com](mailto:hello@hostedscan.com)

# SECURi Website Scan



Website Monitoring

Website Firewall

Malware Removal

Knowledgebase

Support

edge.creatorstudiopro.com



### No Malware Found

Our scanner didn't detect any malware



### Site is not Blacklisted

9 Blacklists checked



#### Redirects to:

<https://edge.creatorstudiopro.com/>

IP address: 99.84.191.10

CDN: Amazon CloudFront

Running on: AmazonS3

CMS: Unknown

Powered by: Unknown

[More Details](#)



Our automated scan did not detect malware on your site. If you still believe that your site has been hacked, sign up for a complete scan, manual audit, and guaranteed malware removal.

## Website Malware & Security

- ✓ No malware detected by scan (Low Risk)
- ✓ No injected spam detected (Low Risk)
- ✓ No defacements detected (Low Risk)
- ✓ No internal server errors detected (Low Risk)



Website Monitoring  
Not detected

[Learn More](#)



Website Firewall  
Firewall Detected

[Explore Sucuri Firewall](#)

## Website Blacklist Status

- ✓ Domain clean by Google Safe Browsing
- ✓ Domain clean by McAfee
- ✓ Domain clean by Sucuri Labs
- ✓ Domain clean by ESET
- ✓ Domain clean by PhishTank
- ✓ Domain clean by Yandex
- ✓ Domain clean by Opera

Your site does not appear to be blacklisted. If you still see security warnings on your site, sign up for a more complete scan, manual audit, and guaranteed blacklist removal.

## Hardening Improvements

### Security Headers

Missing security header for Clickjacking Protection. Alternatively, you can use Content-Security-Policy: frame-ancestors 'none'.

Missing security header to prevent Content Type sniffing.

Missing Strict-Transport-Security security header.

Missing Content-Security-Policy directive. We recommend to add the following CSP directives (you can use default-src if all values are the same): script-src, object-src, base-uri, frame-src

## Hardening Improvements

## Security Headers

Missing security header for [Clickjacking Protection](#). Alternatively, you can use [Content-Security-Policy: frame-ancestors 'none'](#).

Missing security header [to prevent Content Type sniffing](#).

Missing [Strict-Transport-Security security header](#).

Missing [Content-Security-Policy directive](#). We recommend to add the following CSP directives (you can use default-src if all values are the same): script-src, object-src, base-uri, frame-src

# edge.creatorstudiopro.com

Host Profile

Host Issues

## Host Summary

Hostname	IP Address	Hosting Provider	Hosting Type
edge.creatorstudiopro.com			

## Asset Value

Asset Value	Has Authentication	Data Characteristics	Additional Context
	N/A	none	none

## Dimensions

Dimension	Rating	
Certificate Expiration Date	pass	▼
Certificate Subject	pass	▼
Encryption Hash Algorithm	pass	▼
Encryption Key Length	pass	▼
Encryption Protocols	pass	▼
Cotenant IP Hosting	fail	▼
Patching Other	info	▼

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > edge.creatorstudiopro.com

## SSL Report: edge.creatorstudiopro.com

Assessed on: Wed, 14 Feb 2024 14:17:08 UTC | [Hide](#) | [Clear cache](#)

[Scan Another >>](#)

	Server	Test time	Grade
1	<a href="#">65.8.161.120</a> server-65-8-161-120.sfo53.r.cloudfront.net Ready	Wed, 14 Feb 2024 14:04:51 UTC Duration: 61.135 sec	A
2	<a href="#">2600:9000:2146:2600:1b:f8c3:4240:93a1</a> Ready	Wed, 14 Feb 2024 14:05:53 UTC Duration: 61.586 sec	A
3	<a href="#">2600:9000:2146:6200:1b:f8c3:4240:93a1</a> Ready	Wed, 14 Feb 2024 14:06:54 UTC Duration: 61.660 sec	A
4	<a href="#">2600:9000:2146:5a00:1b:f8c3:4240:93a1</a> Ready	Wed, 14 Feb 2024 14:07:56 UTC Duration: 61.92 sec	A
5	<a href="#">2600:9000:2146:3600:1b:f8c3:4240:93a1</a> Ready	Wed, 14 Feb 2024 14:08:57 UTC Duration: 61.91 sec	A
6	<a href="#">2600:9000:2146:7600:1b:f8c3:4240:93a1</a> Ready	Wed, 14 Feb 2024 14:09:58 UTC Duration: 61.465 sec	A
7	<a href="#">2600:9000:2146:4a00:1b:f8c3:4240:93a1</a> Ready	Wed, 14 Feb 2024 14:10:59 UTC Duration: 61.532 sec	A
8	<a href="#">65.8.161.65</a> server-65-8-161-65.sfo53.r.cloudfront.net Ready	Wed, 14 Feb 2024 14:12:01 UTC Duration: 61.816 sec	A

# OWASP ZAP Scan Report

Target: <https://edge.creatorstudiopro.com/>

All scanned sites: <https://edge.creatorstudiopro.com>

Javascript included from: <https://app2.creatorstudiopro.com> <https://connect.facebook.net> <https://www.google-analytics.com>  
<https://www.googletagmanager.com> <https://apis.google.com> <https://edge.creatorstudiopro.com>

Generated on Wed, 28 Feb 2024 18:48:12

ZAP Version: 2.14.0

## Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	4
Informational	3

## Alerts

Name	Risk Level	Number of Instances
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	4
<a href="#">Missing Anti-clickjacking Header</a>	Medium	4
<a href="#">Cross-Domain JavaScript Source File Inclusion</a>	Low	4
<a href="#">Server Leaks Version Information via "Server" HTTP Response Header Field</a>	Low	17
<a href="#">Strict-Transport-Security Header Not Set</a>	Low	16
<a href="#">X-Content-Type-Options Header Missing</a>	Low	16
<a href="#">Re-examine Cache-control Directives</a>	Informational	4
<a href="#">Retrieved from Cache</a>	Informational	3
<a href="#">Session Management Response Identified</a>	Informational	10

## Passing Rules

Name	Rule Type	Threshold	Strength
<a href="#">Verification Request Identified</a>	Passive	MEDIUM	-
<a href="#">Private IP Disclosure</a>	Passive	MEDIUM	-
<a href="#">Session ID in URL Rewrite</a>	Passive	MEDIUM	-
<a href="#">Insecure JSF ViewState</a>	Passive	MEDIUM	-
<a href="#">Vulnerable JS Library (Powered by Retire.js)</a>	Passive	MEDIUM	-



<a href="#">Charset Mismatch</a>	Passive	MEDIUM	-
<a href="#">Cookie No HttpOnly Flag</a>	Passive	MEDIUM	-
<a href="#">Cookie Without Secure Flag</a>	Passive	MEDIUM	-
<a href="#">Content-Type Header Missing</a>	Passive	MEDIUM	-
<a href="#">Application Error Disclosure</a>	Passive	MEDIUM	-
<a href="#">Information Disclosure - Debug Error Messages</a>	Passive	MEDIUM	-
<a href="#">Information Disclosure - Sensitive Information in URL</a>	Passive	MEDIUM	-
<a href="#">Information Disclosure - Sensitive Information in HTTP Referrer Header</a>	Passive	MEDIUM	-
<a href="#">Information Disclosure - Suspicious Comments</a>	Passive	MEDIUM	-
<a href="#">Open Redirect</a>	Passive	MEDIUM	-
<a href="#">Cookie Poisoning</a>	Passive	MEDIUM	-
<a href="#">User Controllable Charset</a>	Passive	MEDIUM	-
<a href="#">WSDL File Detection</a>	Passive	MEDIUM	-
<a href="#">User Controllable HTML Element Attribute (Potential XSS)</a>	Passive	MEDIUM	-
<a href="#">Loosely Scoped Cookie</a>	Passive	MEDIUM	-
<a href="#">Viewstate</a>	Passive	MEDIUM	-
<a href="#">Directory Browsing</a>	Passive	MEDIUM	-
<a href="#">Heartbleed OpenSSL Vulnerability (Indicative)</a>	Passive	MEDIUM	-
<a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a>	Passive	MEDIUM	-
<a href="#">X-Backend-Server Header Information Leak</a>	Passive	MEDIUM	-
<a href="#">Secure Pages Include Mixed Content</a>	Passive	MEDIUM	-
<a href="#">HTTP to HTTPS Insecure Transition in Form Post</a>	Passive	MEDIUM	-
<a href="#">HTTPS to HTTP Insecure Transition in Form Post</a>	Passive	MEDIUM	-
<a href="#">User Controllable JavaScript Event (XSS)</a>	Passive	MEDIUM	-
<a href="#">Big Redirect Detected (Potential Sensitive Information Leak)</a>	Passive	MEDIUM	-
<a href="#">X-ChromeLogger-Data (XCOLD) Header Information Leak</a>	Passive	MEDIUM	-
<a href="#">Cookie without SameSite Attribute</a>	Passive	MEDIUM	-
<a href="#">CSP</a>	Passive	MEDIUM	-
<a href="#">X-Debug-Token Information Leak</a>	Passive	MEDIUM	-
<a href="#">Username Hash Found</a>	Passive	MEDIUM	-
<a href="#">X-AspNet-Version Response Header</a>	Passive	MEDIUM	-
<a href="#">PII Disclosure</a>	Passive	MEDIUM	-
<a href="#">Script Passive Scan Rules</a>	Passive	MEDIUM	-
<a href="#">Stats Passive Scan Rule</a>	Passive	MEDIUM	-
<a href="#">Absence of Anti-CSRF Tokens</a>	Passive	MEDIUM	-
<a href="#">Timestamp Disclosure</a>	Passive	MEDIUM	-
<a href="#">Hash Disclosure</a>	Passive	MEDIUM	-
<a href="#">Cross-Domain Misconfiguration</a>	Passive	MEDIUM	-
<a href="#">Weak Authentication Method</a>	Passive	MEDIUM	-
<a href="#">Reverse Tabnabbing</a>	Passive	MEDIUM	-
<a href="#">Modern Web Application</a>	Passive	MEDIUM	-
<a href="#">Authentication Request Identified</a>	Passive	MEDIUM	-

## Alert Detail

Medium	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	<a href="https://edge.creatorstudiopro.com/">https://edge.creatorstudiopro.com/</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/csp/site.webmanifest">https://edge.creatorstudiopro.com/csp/site.webmanifest</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/privacy-terms/">https://edge.creatorstudiopro.com/privacy-terms/</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/sitemap.xml">https://edge.creatorstudiopro.com/sitemap.xml</a>
Method	GET
Parameter	
Attack	
Evidence	
Instances	4
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy">https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy</a> <a href="https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html</a> <a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://w3c.github.io/webappsec-csp/">https://w3c.github.io/webappsec-csp/</a> <a href="https://web.dev/articles/csp">https://web.dev/articles/csp</a> <a href="https://caniuse.com/#feat=contentsecuritypolicy">https://caniuse.com/#feat=contentsecuritypolicy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10038</a>
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	<a href="https://edge.creatorstudiopro.com/">https://edge.creatorstudiopro.com/</a>
Method	GET
Parameter	x-frame-options

Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/csp/site.webmanifest">https://edge.creatorstudiopro.com/csp/site.webmanifest</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/privacy-terms/">https://edge.creatorstudiopro.com/privacy-terms/</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/sitemap.xml">https://edge.creatorstudiopro.com/sitemap.xml</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Instances	4
Solution	<p>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.</p> <p>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.</p>
Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a>
CWE Id	<a href="#">1021</a>
WASC Id	15
Plugin Id	<a href="#">10020</a>

**Low Cross-Domain JavaScript Source File Inclusion**

Description	The page includes one or more script files from a third-party domain.
URL	<a href="https://edge.creatorstudiopro.com/">https://edge.creatorstudiopro.com/</a>
Method	GET
Parameter	https://apis.google.com/js/client.js?onload=handleClientLoad
Attack	
Evidence	<script src="https://apis.google.com/js/client.js?onload=handleClientLoad"></script>
URL	<a href="https://edge.creatorstudiopro.com/csp/site.webmanifest">https://edge.creatorstudiopro.com/csp/site.webmanifest</a>
Method	GET
Parameter	https://apis.google.com/js/client.js?onload=handleClientLoad
Attack	
Evidence	<script src="https://apis.google.com/js/client.js?onload=handleClientLoad"></script>
URL	<a href="https://edge.creatorstudiopro.com/privacy-terms/">https://edge.creatorstudiopro.com/privacy-terms/</a>
Method	GET

Parameter	https://apis.google.com/js/client.js?onload=handleClientLoad
Attack	
Evidence	<script src="https://apis.google.com/js/client.js?onload=handleClientLoad"></script>
URL	<a href="https://edge.creatorstudiopro.com/sitemap.xml">https://edge.creatorstudiopro.com/sitemap.xml</a>
Method	GET
Parameter	https://apis.google.com/js/client.js?onload=handleClientLoad
Attack	
Evidence	<script src="https://apis.google.com/js/client.js?onload=handleClientLoad"></script>
Instances	4
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	<a href="#">829</a>
WASC Id	15
Plugin Id	<a href="#">10017</a>

**Low Server Leaks Version Information via "Server" HTTP Response Header Field**

Description The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

URL	<a href="https://edge.creatorstudiopro.com/">https://edge.creatorstudiopro.com/</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/0.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/0.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/1.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/1.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/13.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/13.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/15.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/15.8e2150ae.chunk.js</a>
Method	GET
Parameter	

Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/18.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/18.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/2.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/2.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/6.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/6.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/9.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/9.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/csp/site.webmanifest">https://edge.creatorstudiopro.com/csp/site.webmanifest</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/FileAPI.exif.js">https://edge.creatorstudiopro.com/FileAPI.exif.js</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/FileAPI.js">https://edge.creatorstudiopro.com/FileAPI.js</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/index/index_bundle.8e2150ae.js">https://edge.creatorstudiopro.com/index/index_bundle.8e2150ae.js</a>
Method	GET
Parameter	
Attack	

Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/md5.js">https://edge.creatorstudiopro.com/md5.js</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/robots.txt">https://edge.creatorstudiopro.com/robots.txt</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://edge.creatorstudiopro.com/sitemap.xml">https://edge.creatorstudiopro.com/sitemap.xml</a>
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
URL	<a href="https://www.google-analytics.com/analytics.js">https://www.google-analytics.com/analytics.js</a>
Method	GET
Parameter	
Attack	
Evidence	Golfe2
Instances	17
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	<a href="https://httpd.apache.org/docs/current/mod/core.html#servertokens">https://httpd.apache.org/docs/current/mod/core.html#servertokens</a> <a href="https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)">https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)</a> <a href="https://www.troyhunt.com/shhh-dont-let-your-response-headers/">https://www.troyhunt.com/shhh-dont-let-your-response-headers/</a>
CWE Id	<a href="#">200</a>
WASC Id	13
Plugin Id	<a href="#">10036</a>

**Low** **Strict-Transport-Security Header Not Set**

Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	<a href="https://edge.creatorstudiopro.com/">https://edge.creatorstudiopro.com/</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/0.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/0.8e2150ae.chunk.js</a>
Method	GET

Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/1.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/1.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/13.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/13.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/15.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/15.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/18.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/18.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/2.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/2.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/6.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/6.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/9.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/9.8e2150ae.chunk.js</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/csp/site.webmanifest">https://edge.creatorstudiopro.com/csp/site.webmanifest</a>
Method	GET

Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/FileAPI.exif.js">https://edge.creatorstudiopro.com/FileAPI.exif.js</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/FileAPI.js">https://edge.creatorstudiopro.com/FileAPI.js</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/index/index_bundle.8e2150ae.js">https://edge.creatorstudiopro.com/index/index_bundle.8e2150ae.js</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/md5.js">https://edge.creatorstudiopro.com/md5.js</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/robots.txt">https://edge.creatorstudiopro.com/robots.txt</a>
Method	GET
Parameter	
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/sitemap.xml">https://edge.creatorstudiopro.com/sitemap.xml</a>
Method	GET
Parameter	
Attack	
Evidence	
Instances	16
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	<a href="https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html</a> <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a> <a href="https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security">https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security</a> <a href="https://caniuse.com/stricttransportsecurity">https://caniuse.com/stricttransportsecurity</a> <a href="https://datatracker.ietf.org/doc/html/rfc6797">https://datatracker.ietf.org/doc/html/rfc6797</a>
CWE Id	<a href="#">319</a>
WASC Id	15



Plugin Id	<a href="#">10035</a>
<b>Low</b>	<b>X-Content-Type-Options Header Missing</b>
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	<a href="https://edge.creatorstudiopro.com/">https://edge.creatorstudiopro.com/</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/0.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/0.8e2150ae.chunk.js</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/1.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/1.8e2150ae.chunk.js</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/13.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/13.8e2150ae.chunk.js</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/15.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/15.8e2150ae.chunk.js</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/18.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/18.8e2150ae.chunk.js</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/2.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/2.8e2150ae.chunk.js</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

URL	<a href="https://edge.creatorstudiopro.com/6.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/6.8e2150ae.chunk.js</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/9.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/9.8e2150ae.chunk.js</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/csp/site.webmanifest">https://edge.creatorstudiopro.com/csp/site.webmanifest</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/FileAPI.exif.js">https://edge.creatorstudiopro.com/FileAPI.exif.js</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/FileAPI.js">https://edge.creatorstudiopro.com/FileAPI.js</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/index/index_bundle.8e2150ae.js">https://edge.creatorstudiopro.com/index/index_bundle.8e2150ae.js</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/md5.js">https://edge.creatorstudiopro.com/md5.js</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	<a href="https://edge.creatorstudiopro.com/privacy-terms/">https://edge.creatorstudiopro.com/privacy-terms/</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

URL	<a href="https://edge.creatorstudiopro.com/sitemap.xml">https://edge.creatorstudiopro.com/sitemap.xml</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Instances	16
Solution	<p>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.</p> <p>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.</p>
Reference	<a href="https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)">https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)</a> <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10021</a>

<b>Informational</b>	<b>Re-examine Cache-control Directives</b>
----------------------	--

Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	<a href="https://edge.creatorstudiopro.com/">https://edge.creatorstudiopro.com/</a>
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=0, s-maxage=2
URL	<a href="https://edge.creatorstudiopro.com/csp/site.webmanifest">https://edge.creatorstudiopro.com/csp/site.webmanifest</a>
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=0, s-maxage=2
URL	<a href="https://edge.creatorstudiopro.com/privacy-terms/">https://edge.creatorstudiopro.com/privacy-terms/</a>
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=0, s-maxage=2
URL	<a href="https://edge.creatorstudiopro.com/sitemap.xml">https://edge.creatorstudiopro.com/sitemap.xml</a>
Method	GET
Parameter	cache-control
Attack	
Evidence	public, max-age=0, s-maxage=2
Instances	4
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching">https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching</a>

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control>  
<https://grayduck.mn/2021/09/13/cache-control-recommendations/>

CWE Id	<a href="#">525</a>
WASC Id	13
Plugin Id	<a href="#">10015</a>

<b>Informational</b>	<b>Retrieved from Cache</b>
----------------------	-----------------------------

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

URL	<a href="https://edge.creatorstudiopro.com/1.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/1.8e2150ae.chunk.js</a>
-----	---

Method	GET
--------	-----

Parameter	
-----------	--

Attack	
--------	--

Evidence	Hit from cloudfront
----------	---------------------

URL	<a href="https://edge.creatorstudiopro.com/6.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/6.8e2150ae.chunk.js</a>
-----	---

Method	GET
--------	-----

Parameter	
-----------	--

Attack	
--------	--

Evidence	Hit from cloudfront
----------	---------------------

URL	<a href="https://edge.creatorstudiopro.com/9.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/9.8e2150ae.chunk.js</a>
-----	---

Method	GET
--------	-----

Parameter	
-----------	--

Attack	
--------	--

Evidence	Hit from cloudfront
----------	---------------------

Instances	3
-----------	---

Solution	<p>Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:</p> <p>Cache-Control: no-cache, no-store, must-revalidate, private</p> <p>Pragma: no-cache</p> <p>Expires: 0</p> <p>This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.</p>
----------	--

Reference	<a href="https://tools.ietf.org/html/rfc7234">https://tools.ietf.org/html/rfc7234</a> <a href="https://tools.ietf.org/html/rfc7231">https://tools.ietf.org/html/rfc7231</a> <a href="https://www.rfc-editor.org/rfc/rfc9110.html">https://www.rfc-editor.org/rfc/rfc9110.html</a>
-----------	---

CWE Id	
--------	--

WASC Id	
---------	--

Plugin Id	<a href="#">10050</a>
-----------	-----------------------

<b>Informational</b>	<b>Session Management Response Identified</b>
----------------------	---

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	<a href="https://edge.creatorstudiopro.com/">https://edge.creatorstudiopro.com/</a>
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.2.1848664738.1709146067
URL	<a href="https://edge.creatorstudiopro.com/">https://edge.creatorstudiopro.com/</a>
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.2.1497283783.1709146067
URL	<a href="https://edge.creatorstudiopro.com/0.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/0.8e2150ae.chunk.js</a>
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.2.1848664738.1709146067
URL	<a href="https://edge.creatorstudiopro.com/0.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/0.8e2150ae.chunk.js</a>
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.2.1497283783.1709146067
URL	<a href="https://edge.creatorstudiopro.com/9.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/9.8e2150ae.chunk.js</a>
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.2.2066563850.1709146076
URL	<a href="https://edge.creatorstudiopro.com/9.8e2150ae.chunk.js">https://edge.creatorstudiopro.com/9.8e2150ae.chunk.js</a>
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.2.1587924549.1709146076
URL	<a href="https://edge.creatorstudiopro.com/FileAPI.js">https://edge.creatorstudiopro.com/FileAPI.js</a>
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.2.1848664738.1709146067
URL	<a href="https://edge.creatorstudiopro.com/FileAPI.js">https://edge.creatorstudiopro.com/FileAPI.js</a>
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.2.1497283783.1709146067

URL	<a href="https://edge.creatorstudiopro.com/static/media">https://edge.creatorstudiopro.com/static/media</a>
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.2.75141386.1709146064
URL	<a href="https://edge.creatorstudiopro.com/static/media/CreatorStudioLogo.93e196b9.svg">https://edge.creatorstudiopro.com/static/media/CreatorStudioLogo.93e196b9.svg</a>
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.2.96764991.1709146064
Instances	10
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	<a href="https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id">https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10112</a>

# Website Vulnerability Scanner Report

✓ <https://edge.creatorstudiopro.com>

⚠ The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. [Upgrade](#) to run Deep scans with 40+ tests and detect more vulnerabilities.

## Summary

### Overall risk level:

Medium

### Risk ratings:



### Scan information:

Start time: Feb 28, 2024 / 20:28:11  
 Finish time: Feb 28, 2024 / 20:28:49  
 Scan duration: 38 sec  
 Tests performed: 18/18  
 Scan status: Finished

## Findings

### 🚩 Vulnerabilities found for server-side software

UNCONFIRMED ⓘ

Risk Level	CVSS	CVE	Summary	Affected software
●	4.3	<a href="#">CVE-2016-10735</a>	In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.	bootstrap 3.3.6
●	4.3	<a href="#">CVE-2018-14040</a>	In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.	bootstrap 3.3.6
●	4.3	<a href="#">CVE-2018-14042</a>	In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.	bootstrap 3.3.6
●	4.3	<a href="#">CVE-2018-20676</a>	In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.	bootstrap 3.3.6
●	4.3	<a href="#">CVE-2018-20677</a>	In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.	bootstrap 3.3.6

#### ▼ Details

#### Risk description:

The risk is that an attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

#### Recommendation:

We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

#### Classification:

CWE : [CWE-1026](#)  
 OWASP Top 10 - 2013 : [A9 - Using Components with Known Vulnerabilities](#)  
 OWASP Top 10 - 2017 : [A9 - Using Components with Known Vulnerabilities](#)

### 🚩 Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence

<a href="https://edge.creatorstudiopro.com">https://edge.creatorstudiopro.com</a>	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response.
---	---

▼ Details

**Risk description:**  
The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the **Referer** header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

**Recommendation:**  
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value **no-referrer** of this header instructs the browser to omit the Referer header entirely.

**References:**  
[https://developer.mozilla.org/en-US/docs/Web/Security/Referer\\_header:\\_privacy\\_and\\_security\\_concerns](https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns)

**Classification:**  
CWE : [CWE-693](#)  
OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)  
OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

## 🚩 Missing security header: Content-Security-Policy

CONFIRMED

URL	Evidence
<a href="https://edge.creatorstudiopro.com">https://edge.creatorstudiopro.com</a>	Response does not include the HTTP Content-Security-Policy security header or meta tag

▼ Details

**Risk description:**  
The risk is that if the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

**Recommendation:**  
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

**References:**  
[https://cheatsheetseries.owasp.org/cheatsheets/Content\\_Security\\_Policy\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html)  
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy>

**Classification:**  
CWE : [CWE-693](#)  
OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)  
OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

## 🚩 Missing security header: X-Content-Type-Options

CONFIRMED

URL	Evidence
<a href="https://edge.creatorstudiopro.com">https://edge.creatorstudiopro.com</a>	Response headers do not include the X-Content-Type-Options HTTP security header

▼ Details

**Risk description:**  
The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

**Recommendation:**  
We recommend setting the X-Content-Type-Options header such as **X-Content-Type-Options: nosniff**.

**References:**  
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options>

**Classification:**  
CWE : [CWE-693](#)  
OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)  
OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)



## Missing security header: Strict-Transport-Security

CONFIRMED

URL	Evidence
<a href="https://edge.creatorstudio.pro">https://edge.creatorstudio.pro</a>	Response headers do not include the HTTP Strict-Transport-Security header

### Details

#### Risk description:

The risk is that lack of this header permits an attacker to force a victim user to initiate a clear-text HTTP connection to the server, thus opening the possibility to eavesdrop on the network traffic and extract sensitive information (e.g. session cookies).

#### Recommendation:

The Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows:

```
Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]
```

The parameter `max-age` gives the time frame for requirement of HTTPS in seconds and should be chosen quite high, e.g. several months. A value below 7776000 is considered as too low by this scanner check.

The flag `includeSubDomains` defines that the policy applies also for sub domains of the sender of the response.

#### Classification:

CWE : [CWE-693](#)

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

## Server software and technology found

UNCONFIRMED

Software / Version	Category
Amazon Cloudfront	CDN
Amazon S3	CDN
Google Analytics GA4	Analytics
Typekit	Font scripts
Google Tag Manager	Tag managers
Amazon Web Services	PaaS
AWS Certificate Manager	SSL/TLS certificate authorities
Babel	Miscellaneous
Facebook Login	Authentication
Font Awesome 4.6.3	Font scripts
Fourthwall \1	Ecommerce
Bootstrap 3.3.6	UI frameworks
core-js 2.6.12	JavaScript libraries
HTTP/3	Miscellaneous
React	JavaScript frameworks
PWA	Miscellaneous
Webpack	Miscellaneous

### Details

#### Risk description:

The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

**Recommendation:**

We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

**References:**

[https://owasp.org/www-project-web-security-testing-guide/stable/4-Web\\_Application\\_Security\\_Testing/01-Information\\_Gathering/02-Fingerprint\\_Web\\_Server.html](https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html)

**Classification:**

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)  
OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

 Security.txt file is missing

CONFIRMED

**URL**

Missing: <https://edge.creatorstudiopro.com/.well-known/security.txt>

▼ Details

**Risk description:**

We have detected that the server is missing the security.txt file. There is no particular risk in not creating a valid Security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

**Recommendation:**

We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

**References:**

<https://securitytxt.org/>

**Classification:**

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)  
OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

 Website is accessible.

 Nothing was found for client access policies.

 Nothing was found for robots.txt file.

 Nothing was found for use of untrusted certificates.

 Nothing was found for enabled HTTP debug methods.

 Nothing was found for secure communication.

 Nothing was found for directory listing.

 Nothing was found for domain too loose set for cookies.

 Nothing was found for HttpOnly flag of cookie.

🚩 Nothing was found for Secure flag of cookie.

---

🚩 Nothing was found for unsafe HTTP header Content Security Policy.

## Scan coverage information

---

### List of tests performed (18/18)

- ✓ Checking for website accessibility...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ Checking for website technologies...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for client access policies...
- ✓ Checking for robots.txt file...
- ✓ Checking for absence of the security.txt file...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for enabled HTTP debug methods...
- ✓ Checking for secure communication...
- ✓ Checking for directory listing...
- ✓ Checking for domain too loose set for cookies...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for unsafe HTTP header Content Security Policy...

### Scan parameters

Target: https://edge.creatorstudiopro.com  
Scan type: Light  
Authentication: False

### Scan stats

Unique Injection Points Detected:	1
URLs spidered:	6
Total number of HTTP requests:	14
Average time until a response was received:	262ms

# Nmap Scan Report - Scanned at Wed Feb 28 18:47:35 2024

Scan Summary | [edge.creatorstudiopro.com \(18.238.80.70\)](#)

## Scan Summary

Nmap 7.70 was initiated at Wed Feb 28 18:47:35 2024 with these arguments:

```
nmap -v -oX=- --host-timeout=8h -Pn -T4 -sT --webxml --max-retries=1 --open -p0-65535 edge.creatorstudiopro.com
```

Verbosity: 1; Debug level 0

Nmap done at Wed Feb 28 18:49:02 2024; 1 IP address (1 host up) scanned in 86.62 seconds

**18.238.80.70 / edge.creatorstudiopro.com / server-18-238-80-70.jfk52.r.cloudfront.net**

## Address

- 18.238.80.70 (ipv4)

## Hostnames

- edge.creatorstudiopro.com (user)
- server-18-238-80-70.jfk52.r.cloudfront.net (PTR)

## Ports

The 65534 ports scanned but not shown below are in state: **filtered**

- 65534 ports replied with: **no-responses**

Port	State (toggle closed [0]   filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp open	http	syn-ack			
443	tcp open	https	syn-ack			

Misc Metrics (click to expand)

Go to top  
Toggle Closed Ports  
Toggle Filtered Ports