OWASP ZAP Scan Report

Target: https://sms.celloscope.net/

All scanned sites: https://sms.celloscope.net

Javascript included from: https://sms.celloscope.net

Generated on Thu, 13 Jul 2023 05:57:37

ZAP Version: 2.12.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	5
Low	4
Informational	2

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	2
Content Security Policy (CSP) Header Not Set	Medium	20
Cross-Domain Misconfiguration	Medium	23
Missing Anti-clickjacking Header	Medium	4
Vulnerable JS Library	Medium	1
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	12
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	27
Strict-Transport-Security Header Not Set	Low	27
X-Content-Type-Options Header Missing	Low	11
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	12
Re-examine Cache-control Directives	Informational	5

Alert Detail

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including:

	* The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://sms.celloscope.net/36.1fdd0e5bb433292390ba.chunk.js
Method	GET
Parameter	
Attack	
Evidence	<form id="loginform" class="form-horizontal" role="form" #f="ngForm" novalidate>
URL	https://sms.celloscope.net/main.b86f111d6990ff517240.bundle.js
Method	GET
Parameter	
Attack	
Evidence	<form id="loginform" class="form-horizontal" role="form" (keydown)="keyDownFunction($event)">
Instances	2
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

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	https://sms.celloscope.net/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/0/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/0/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/0/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/0/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/0/swp/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/drws/drws/
Method	GET
Parameter	

Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/swp/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/ibu/swp/
Method	GET
Parameter	
Attack	
Evidence	

URL	https://sms.celloscope.net/app/inklusion/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/login
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Instances	20
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 http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

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	https://sms.celloscope.net/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/0.a50ece2320d1b6b80f2c.chunk.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *

URL	https://sms.celloscope.net/36.1fdd0e5bb433292390ba.chunk.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/app/0/drws/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/app/0/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/app/0/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/app/0/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/app/1/drws/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/app/1/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/app/1/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/app/1/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET

Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/app/drws/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/app/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/app/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/app/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/assets/i18n/en.json
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/inline.13f9603286a3ee722dbd.bundle.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/login
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/main.b86f111d6990ff517240.bundle.js
Method	GET
Parameter	
Attack	

Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/robots.txt
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/scripts.44d05a497155b46d33da.bundle.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://sms.celloscope.net/vendor.e3031eb65b3a160781c4.bundle.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Instances	23
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
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

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	https://sms.celloscope.net/
Method	GET
Parameter	X-Frame-Options
Attack	
Evidence	
URL	https://sms.celloscope.net/login
Method	GET
Parameter	X-Frame-Options
Attack	
Evidence	
URL	https://sms.celloscope.net/robots.txt

Method	GET
Parameter	X-Frame-Options
Attack	
Evidence	
URL	https://sms.celloscope.net/sitemap.xml
Method	GET
Parameter	X-Frame-Options
Attack	
Evidence	
Instances	4
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

Medium	**Vulnerable JS Library**
Description	The identified library bootstrap, version 3.4.1 is vulnerable.
URL	https://sms.celloscope.net/scripts.44d05a497155b46d33da.bundle.js
Method	GET
Parameter	
Attack	
Evidence	this.close)};n.VERSION="3.4.1",n.TRANSITION_DURATION=150,n.prototype.close
Instances	1
Solution	Please upgrade to the latest version of bootstrap.
Reference	https://github.com/twbs/bootstrap/issues/20631
CWE Id	829
WASC Id	
Plugin Id	10003

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	https://sms.celloscope.net/app/0/drws/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Drws :-)
URL	https://sms.celloscope.net/app/0/drws/drws/
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: Drws :-)
URL	https://sms.celloscope.net/app/0/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Drws :-)
URL	https://sms.celloscope.net/app/0/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Drws :-)
URL	https://sms.celloscope.net/app/1/drws/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Drws :-)
URL	https://sms.celloscope.net/app/1/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Drws :-)
URL	https://sms.celloscope.net/app/1/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Drws :-)
URL	https://sms.celloscope.net/app/1/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Drws :-)
URL	https://sms.celloscope.net/app/drws/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Drws :-)
URL	https://sms.celloscope.net/app/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Drws :-)
URL	https://sms.celloscope.net/app/drws/drws/drws/drws/

Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Drws :-)
URL	https://sms.celloscope.net/app/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Drws :-)
Instances	12
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037

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	https://sms.celloscope.net/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/0.a50ece2320d1b6b80f2c.chunk.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/36.1fdd0e5bb433292390ba.chunk.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/0/drws/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/0/drws/drws/
Method	GET
Parameter	
Attack	

Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/0/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/0/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/0/swp/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/1/drws/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/1/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/1/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/1/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/1/swp/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/drws/

Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/ibu/swp/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/app/inklusion/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/assets/i18n/en.json
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/inline.13f9603286a3ee722dbd.bundle.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/login
Method	GET
Parameter	

Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/main.b86f111d6990ff517240.bundle.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/robots.txt
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/scripts.44d05a497155b46d33da.bundle.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://sms.celloscope.net/vendor.e3031eb65b3a160781c4.bundle.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
Instances	27
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10036

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	https://sms.celloscope.net/
Method	GET
Parameter	
Attack	

Evidence	
URL	https://sms.celloscope.net/0.a50ece2320d1b6b80f2c.chunk.js
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/36.1fdd0e5bb433292390ba.chunk.js
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/0/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/0/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/0/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/0/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/0/swp/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/drws/drws/

Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/swp/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/ibu/swp/
Method	GET
Parameter	

Attack	
Evidence	
URL	https://sms.celloscope.net/app/inklusion/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/assets/i18n/en.json
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/inline.13f9603286a3ee722dbd.bundle.js
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/login
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/main.b86f111d6990ff517240.bundle.js
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/scripts.44d05a497155b46d33da.bundle.js
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	

URL	https://sms.celloscope.net/vendor.e3031eb65b3a160781c4.bundle.js
Method	GET
Parameter	
Attack	
Evidence	
Instances	27
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

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	https://sms.celloscope.net/
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://sms.celloscope.net/0.a50ece2320d1b6b80f2c.chunk.js
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://sms.celloscope.net/36.1fdd0e5bb433292390ba.chunk.js
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://sms.celloscope.net/assets/i18n/en.json
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://sms.celloscope.net/inline.13f9603286a3ee722dbd.bundle.js
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	

URL	https://sms.celloscope.net/login
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://sms.celloscope.net/main.b86f111d6990ff517240.bundle.js
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://sms.celloscope.net/robots.txt
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://sms.celloscope.net/scripts.44d05a497155b46d33da.bundle.js
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://sms.celloscope.net/sitemap.xml
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://sms.celloscope.net/vendor.e3031eb65b3a160781c4.bundle.js
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
Instances	11
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	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Charset Mismatch (Header Versus Meta Content-Type Charset)**
Description	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set.

	An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.
URL	https://sms.celloscope.net/app/0/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/0/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/0/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/0/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/1/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	

URL	https://sms.celloscope.net/app/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://sms.celloscope.net/app/drws/drws/drws/drws/drws/drws/drws/drws/
Method	GET
Parameter	
Attack	
Evidence	
Instances	12
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011

Informational	**Re-examine Cache-control Directives**
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	https://sms.celloscope.net/
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://sms.celloscope.net/assets/i18n/en.json
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://sms.celloscope.net/login
Method	GET
Parameter	Cache-Control

Attack	
Evidence	
URL	https://sms.celloscope.net/robots.txt
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://sms.celloscope.net/sitemap.xml
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
Instances	5
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	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015