⚡ ZAP Scanning Report

scansione automatica ajax spider master

Site: http://10.0.2.4

Generated on Mon, 13 May 2024 03:46:42

ZAP Version: 2.14.0

ZAP is supported by the [Crash Override Open Source Fellowship](#)

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	3
Content Security Policy (CSP) Header Not Set	Medium	11
Missing Anti-clickjacking Header	Medium	3
Vulnerable JS Library	Medium	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	25
X-Content-Type-Options Header Missing	Low	16
Content-Type Header Missing	Informational	3
Information Disclosure - Suspicious Comments	Informational	2
Modern Web Application	Informational	3
Session Management Response Identified	Informational	5
User Agent Fuzzer	Informational	144

Alert Detail

Medium	Absence of Anti-CSRF Tokens
	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

Description	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	http://10.0.2.4
Method	GET
Attack	
Evidence	<form class="form-inline d-flex">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "inputEmail"].
URL	http://10.0.2.4/
Method	GET
Attack	
Evidence	<form class="form-inline d-flex">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "inputEmail"].
URL	http://10.0.2.4/masteradmin/login.php
Method	GET
Attack	
Evidence	<form class="login100-form validate-form flex-sb flex-w" method="POST" action="">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "ckb1" "password" "username"].
Instances	3
	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 |

| Solution | 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 | https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
https://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	http://10.0.2.4
Method	GET
Attack	
Evidence	
Other Info	
URL	http://10.0.2.4/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://10.0.2.4/css/
Method	GET
Attack	
Evidence	
Other Info	

URL	http://10.0.2.4/favicon.ico	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://10.0.2.4/img/image.png	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://10.0.2.4/masteradmin/fonts/font-awesome-4.7.0/fonts/fontawesome-webfont.ttf?v=4.7.0	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://10.0.2.4/masteradmin/fonts/font-awesome-4.7.0/fonts/fontawesome-webfont.woff2?v=4.7.0	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://10.0.2.4/masteradmin/fonts/font-awesome-4.7.0/fonts/fontawesome-webfont.woff?v=4.7.0	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://10.0.2.4/masteradmin/login.php	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://10.0.2.4/robots.txt	
Method	GET	
Attack		
Evidence		
Other Info		

URL	http://10.0.2.4/sitemap.xml	
Method	GET	
Attack		
Evidence		
Other Info		
Instances	11	
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	

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://10.0.2.4
Method	GET
Attack	
Evidence	
Other Info	
URL	http://10.0.2.4/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://10.0.2.4/masteradmin/login.php
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
	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.
Solution	

	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 jquery, version 3.4.1 is vulnerable.
URL	http://10.0.2.4/vendor/jquery/jquery.min.js
Method	GET
Attack	
Evidence	/*! jQuery v3.4.1
Other Info	CVE-2020-11023 CVE-2020-11022
Instances	1
Solution	Please upgrade to the latest version of jquery.
Reference	https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
CWE Id	829
WASC Id	
Plugin Id	10003

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	http://10.0.2.4
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
URL	http://10.0.2.4/
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
URL	http://10.0.2.4/css
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	

	URL	http://10.0.2.4/css/
	Method	GET
	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
	URL	http://10.0.2.4/css/grayscale.min.css
	Method	GET
	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
	URL	http://10.0.2.4/favicon.ico
	Method	GET
	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
	URL	http://10.0.2.4/img/bg-masthead.jpg
	Method	GET
	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
	URL	http://10.0.2.4/img/bg-signup.jpg
	Method	GET
	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
	URL	http://10.0.2.4/img/image.png
	Method	GET
	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
	URL	http://10.0.2.4/js/grayscale.min.js
	Method	GET
	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
	URL	http://10.0.2.4/masteradmin/fonts/font-awesome-4.7.0/fonts/fontawesome-webfont.ttf?v=4.7.0

Method	GET	
Attack		
Evidence	Apache/2.4.18 (Ubuntu)	
Other Info		
URL	http://10.0.2.4/masteradmin/fonts/font-awesome-4.7.0/fonts/fontawesome-webfont.woff2?v=4.7.0	
Method	GET	
Attack		
Evidence	Apache/2.4.18 (Ubuntu)	
Other Info		
URL	http://10.0.2.4/masteradmin/fonts/font-awesome-4.7.0/fonts/fontawesome-webfont.woff?v=4.7.0	
Method	GET	
Attack		
Evidence	Apache/2.4.18 (Ubuntu)	
Other Info		
URL	http://10.0.2.4/masteradmin/fonts/raleway/Raleway-Medium.ttf	
Method	GET	
Attack		
Evidence	Apache/2.4.18 (Ubuntu)	
Other Info		
URL	http://10.0.2.4/masteradmin/login.php	
Method	GET	
Attack		
Evidence	Apache/2.4.18 (Ubuntu)	
Other Info		
URL	http://10.0.2.4/robots.txt	
Method	GET	
Attack		
Evidence	Apache/2.4.18 (Ubuntu)	
Other Info		
URL	http://10.0.2.4/sitemap.xml	
Method	GET	
Attack		
Evidence	Apache/2.4.18 (Ubuntu)	
Other Info		
URL	http://10.0.2.4/vendor/bootstrap/css/bootstrap.min.css	
Method	GET	

	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
URL		http://10.0.2.4/vendor/bootstrap/js/bootstrap.bundle.min.js
	Method	GET
	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
URL		http://10.0.2.4/vendor/fontawesome-free/css/all.min.css
	Method	GET
	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
URL		http://10.0.2.4/vendor/fontawesome-free/webfonts/fa-brands-400.woff2
	Method	GET
	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
URL		http://10.0.2.4/vendor/fontawesome-free/webfonts/fa-regular-400.woff2
	Method	GET
	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
URL		http://10.0.2.4/vendor/fontawesome-free/webfonts/fa-solid-900.woff2
	Method	GET
	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
URL		http://10.0.2.4/vendor/jquery-easing/jquery.easing.min.js
	Method	GET
	Attack	
	Evidence	Apache/2.4.18 (Ubuntu)
	Other Info	
URL		http://10.0.2.4/vendor/jquery/jquery.min.js
	Method	GET
	Attack	

Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
Instances	25
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	200
WASC Id	13
Plugin Id	10036

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://10.0.2.4
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://10.0.2.4/
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://10.0.2.4/css/grayscale.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://10.0.2.4/img/bg-masthead.jpg
Method	GET
Attack	
Evidence	
Other	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

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.	
URL	http://10.0.2.4/img/bg-signup.jpg	
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://10.0.2.4/js/grayscale.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://10.0.2.4/masteradmin/fonts/raleway/Raleway-Medium.ttf	
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://10.0.2.4/masteradmin/login.php	
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://10.0.2.4/vendor/bootstrap/css/bootstrap.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://10.0.2.4/vendor/bootstrap/js/bootstrap.bundle.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://10.0.2.4/vendor/fontawesome-free/css/all.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://10.0.2.4/vendor/fontawesome-free/webfonts/fa-brands-400.woff2
	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://10.0.2.4/vendor/fontawesome-free/webfonts/fa-regular-400.woff2
	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://10.0.2.4/vendor/fontawesome-free/webfonts/fa-solid-900.woff2
	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://10.0.2.4/vendor/jquery-easing/jquery.easing.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://10.0.2.4/vendor/jquery/jquery.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.

Instances	16
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

Informational	Content-Type Header Missing
Description	The Content-Type header was either missing or empty.
URL	http://10.0.2.4/vendor/fontawesome-free/webfonts/fa-brands-400.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/fontawesome-free/webfonts/fa-regular-400.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/fontawesome-free/webfonts/fa-solid-900.woff2
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
Solution	Ensure each page is setting the specific and appropriate content-type value for the content being delivered.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer /compatibility/gg622941(v=vs.85)
CWE Id	345
WASC Id	12
Plugin Id	10019

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://10.0.2.4/vendor/bootstrap/js/bootstrap.bundle.min.js
Method	GET

Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "! function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require ("jquery")):"function"==typeof define&&defi", see evidence field for the suspicious comment /snippet.
URL	http://10.0.2.4/vendor/jquery/jquery.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.
Instances	2
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10027

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://10.0.2.4
Method	GET
Attack	
Evidence	That's who we are.
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://10.0.2.4/
Method	GET
Attack	
Evidence	That's who we are.
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://10.0.2.4/masteradmin/login.php
Method	GET
Attack	
Evidence	 Forgot Password?
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Instances	3
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	

WASC Id	
Plugin Id	10109

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://10.0.2.4/css
Method	GET
Attack	
Evidence	pvl7lhj7d26rieks43840macp2
Other Info	cookie:PHPSESSID
URL	http://10.0.2.4/masteradmin
Method	GET
Attack	
Evidence	pvl7lhj7d26rieks43840macp2
Other Info	cookie:PHPSESSID
URL	http://10.0.2.4/masteradmin/fonts/font-awesome-4.7.0/fonts
Method	GET
Attack	
Evidence	pvl7lhj7d26rieks43840macp2
Other Info	cookie:PHPSESSID
URL	http://10.0.2.4/masteradmin/fonts/font-awesome-4.7.0/fonts/fontawesome-webfont.ttf?v=4.7.0
Method	GET
Attack	
Evidence	pvl7lhj7d26rieks43840macp2
Other Info	cookie:PHPSESSID
URL	http://10.0.2.4/masteradmin/fonts/font-awesome-4.7.0/fonts/fontawesome-webfont.woff?v=4.7.0
Method	GET
Attack	
Evidence	pvl7lhj7d26rieks43840macp2
Other Info	cookie:PHPSESSID
Instances	5
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

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://10.0.2.4/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://10.0.2.4/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://10.0.2.4/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://10.0.2.4/css
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://10.0.2.4/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://10.0.2.4/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://10.0.2.4/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://10.0.2.4/css
	Method	GET
	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
	Evidence	
	Other Info	
URL		http://10.0.2.4/css
	Method	GET
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
	Evidence	
	Other Info	
URL		http://10.0.2.4/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://10.0.2.4/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://10.0.2.4/css
	Method	GET
	Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
	Evidence	
	Other Info	
URL		http://10.0.2.4/img
	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
	Evidence	
	Other Info	
URL		http://10.0.2.4/img
	Method	GET

Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)	
Evidence		
Other Info		
URL	http://10.0.2.4/img	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	
Evidence		
Other Info		
URL	http://10.0.2.4/img	
Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko	
Evidence		
Other Info		
URL	http://10.0.2.4/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://10.0.2.4/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://10.0.2.4/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://10.0.2.4/img	
Method	GET	
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	
Evidence		
Other Info		
URL	http://10.0.2.4/img	
Method	GET	
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)	

Evidence	
Other Info	
URL	http://10.0.2.4/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://10.0.2.4/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://10.0.2.4/img
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://10.0.2.4/js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://10.0.2.4/js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://10.0.2.4/js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://10.0.2.4/js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko

	Evidence	
	Other Info	
URL		http://10.0.2.4/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://10.0.2.4/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://10.0.2.4/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://10.0.2.4/js
	Method	GET
	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
	Evidence	
	Other Info	
URL		http://10.0.2.4/js
	Method	GET
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
	Evidence	
	Other Info	
URL		http://10.0.2.4/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://10.0.2.4/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://10.0.2.4/js
	Method	GET
	Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor
	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor
	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor
	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor
	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://10.0.2.4/vendor
	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://10.0.2.4/vendor	
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://10.0.2.4/vendor	
Method	GET	
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	
Evidence		
Other Info		
URL	http://10.0.2.4/vendor	
Method	GET	
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)	
Evidence		
Other Info		
URL	http://10.0.2.4/vendor	
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://10.0.2.4/vendor	
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://10.0.2.4/vendor	
Method	GET	
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)	
Evidence		
Other Info		
URL	http://10.0.2.4/vendor/bootstrap	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	
Evidence		

Other Info	
URL	http://10.0.2.4/vendor/bootstrap
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap
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://10.0.2.4/vendor/bootstrap
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://10.0.2.4/vendor/bootstrap
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://10.0.2.4/vendor/bootstrap
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	

Other Info	
URL	http://10.0.2.4/vendor/bootstrap
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap
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://10.0.2.4/vendor/bootstrap
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://10.0.2.4/vendor/bootstrap
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other	

Info	
URL	http://10.0.2.4/vendor/bootstrap/css
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap/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://10.0.2.4/vendor/bootstrap/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://10.0.2.4/vendor/bootstrap/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://10.0.2.4/vendor/bootstrap/css
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap/css
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap/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://10.0.2.4/vendor/bootstrap/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://10.0.2.4/vendor/bootstrap/css
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap/js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap/js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap/js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap/js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap/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://10.0.2.4/vendor/bootstrap/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://10.0.2.4/vendor/bootstrap/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://10.0.2.4/vendor/bootstrap/js
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap/js
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/bootstrap/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://10.0.2.4/vendor/bootstrap/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://10.0.2.4/vendor/bootstrap/js
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	

URL	http://10.0.2.4/vendor/fontawesome-free
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/fontawesome-free
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/fontawesome-free
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/fontawesome-free
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/fontawesome-free
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://10.0.2.4/vendor/fontawesome-free
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://10.0.2.4/vendor/fontawesome-free
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://10.0.2.4/vendor/fontawesome-free

	Method	GET
	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/fontawesome-free
	Method	GET
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/fontawesome-free
	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://10.0.2.4/vendor/fontawesome-free
	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://10.0.2.4/vendor/fontawesome-free
	Method	GET
	Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/fontawesome-free/css
	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/fontawesome-free/css
	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/fontawesome-free/css

	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/fontawesome-free/css
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/fontawesome-free/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://10.0.2.4/vendor/fontawesome-free/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://10.0.2.4/vendor/fontawesome-free/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://10.0.2.4/vendor/fontawesome-free/css
	Method	GET
	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/fontawesome-free/css
	Method	GET
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/fontawesome-free/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://10.0.2.4/vendor/fontawesome-free/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://10.0.2.4/vendor/fontawesome-free/css	
Method	GET	
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)	
Evidence		
Other Info		
URL	http://10.0.2.4/vendor/fontawesome-free/webfonts	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	
Evidence		
Other Info		
URL	http://10.0.2.4/vendor/fontawesome-free/webfonts	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)	
Evidence		
Other Info		
URL	http://10.0.2.4/vendor/fontawesome-free/webfonts	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	
Evidence		
Other Info		
URL	http://10.0.2.4/vendor/fontawesome-free/webfonts	
Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko	
Evidence		
Other Info		
URL	http://10.0.2.4/vendor/fontawesome-free/webfonts	
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://10.0.2.4/vendor/fontawesome-free/webfonts
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://10.0.2.4/vendor/fontawesome-free/webfonts
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://10.0.2.4/vendor/fontawesome-free/webfonts
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/fontawesome-free/webfonts
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://10.0.2.4/vendor/fontawesome-free/webfonts
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://10.0.2.4/vendor/fontawesome-free/webfonts
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://10.0.2.4/vendor/fontawesome-free/webfonts
Method	GET

	Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/jquery
	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/jquery
	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/jquery
	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/jquery
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/jquery
	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://10.0.2.4/vendor/jquery
	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://10.0.2.4/vendor/jquery
	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://10.0.2.4/vendor/jquery	
Method	GET	
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	
Evidence		
Other Info		
URL	http://10.0.2.4/vendor/jquery	
Method	GET	
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)	
Evidence		
Other Info		
URL	http://10.0.2.4/vendor/jquery	
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://10.0.2.4/vendor/jquery	
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://10.0.2.4/vendor/jquery	
Method	GET	
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)	
Evidence		
Other Info		
URL	http://10.0.2.4/vendor/jquery-easing	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	
Evidence		
Other Info		
URL	http://10.0.2.4/vendor/jquery-easing	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)	

	Evidence	
	Other Info	
	URL	http://10.0.2.4/vendor/jquery-easing
	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
	Evidence	
	Other Info	
	URL	http://10.0.2.4/vendor/jquery-easing
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
	Evidence	
	Other Info	
	URL	http://10.0.2.4/vendor/jquery-easing
	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://10.0.2.4/vendor/jquery-easing
	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://10.0.2.4/vendor/jquery-easing
	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://10.0.2.4/vendor/jquery-easing
	Method	GET
	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
	Evidence	
	Other Info	
	URL	http://10.0.2.4/vendor/jquery-easing
	Method	GET
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)

	Evidence	
	Other Info	
URL		http://10.0.2.4/vendor/jquery-easing
	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://10.0.2.4/vendor/jquery-easing
	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://10.0.2.4/vendor/jquery-easing
	Method	GET
	Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
	Evidence	
	Other Info	
Instances		144
Solution		
Reference		https://owasp.org/wstg
CWE Id		
WASC Id		
Plugin Id		10104