

ZAP Scanning Report

Summary of Alerts

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

Alert Detail

Low (Medium)

X-Content-Type-Options Header Missing

Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://localhost:4200/
Method	GET
Parameter	X-Content-Type-Options
URL	http://localhost:4200/main.bundle.js
Method	GET
Parameter	X-Content-Type-Options
URL	http://localhost:4200
Method	GET
Parameter	X-Content-Type-Options
URL	http://localhost:4200/inline.bundle.js
Method	GET
Parameter	X-Content-Type-Options
URL	http://localhost:4200/styles.bundle.js
Method	GET
Parameter	X-Content-Type-Options
Instances	5
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.
Other information	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.
Reference	At "High" threshold this scanner will not alert on client or server error responses. http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx

CWE Id	https://www.owasp.org/index.php/List_of_useful_HTTP_headers
WASC Id	16
Source ID	15
	3
Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	http://localhost:4200
Method	GET
Parameter	X-XSS-Protection
URL	http://localhost:4200/robots.txt
Method	GET
Parameter	X-XSS-Protection
URL	http://localhost:4200/sitemap.xml
Method	GET
Parameter	X-XSS-Protection
URL	http://localhost:4200/
Method	GET
Parameter	X-XSS-Protection
Instances	4
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	<p>The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it:</p> <p>X-XSS-Protection: 1; mode=block</p> <p>X-XSS-Protection: 1; report=http://www.example.com/xss</p> <p>The following values would disable it:</p> <p>X-XSS-Protection: 0</p> <p>The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).</p> <p>Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).</p>
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3
Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early

	2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://localhost:8000/static/admin/css/login.css
Method	GET
Parameter	X-Content-Type-Options
URL	http://localhost:8000/admin
Method	GET
Parameter	X-Content-Type-Options
URL	http://localhost:8000/admin/login/?next=/admin/
Method	GET
Parameter	X-Content-Type-Options
URL	http://localhost:8000/static/admin/css/base.css
Method	GET
Parameter	X-Content-Type-Options
Instances	4
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.
Other information	<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> <p>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.</p>
Reference	<p>At "High" threshold this scanner will not alert on client or server error responses.</p> <p>http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx</p> <p>https://www.owasp.org/index.php/List_of_useful_HTTP_headers</p>
CWE Id	16
WASC Id	15
Source ID	3
Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	http://localhost:8000/sitemap.xml
Method	GET
Parameter	X-XSS-Protection
URL	http://localhost:8000/admin
Method	GET
Parameter	X-XSS-Protection
URL	http://localhost:8000/robots.txt

Method	GET
Parameter	X-XSS-Protection
URL	http://localhost:8000/admin/login/?next=/admin/
Method	GET
Parameter	X-XSS-Protection
URL	http://localhost:8000/admin/login/?next=/admin/
Method	POST
Parameter	X-XSS-Protection
Instances	5
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	<p>The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it:</p> <p>X-XSS-Protection: 1; mode=block</p> <p>X-XSS-Protection: 1; report=http://www.example.com/xss</p> <p>The following values would disable it:</p> <p>X-XSS-Protection: 0</p> <p>The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).</p> <p>Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).</p>
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3
Low (Medium)	
Description	Cookie No HttpOnly Flag A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://localhost:8000/admin/login/?next=/admin/
Method	GET
Parameter	csrftoken
Evidence	Set-Cookie: csrftoken
URL	http://localhost:8000/admin
Method	GET
Parameter	csrftoken
Evidence	Set-Cookie: csrftoken

Instances	2
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	http://www.owasp.org/index.php/HttpOnly
CWE Id	16
WASC Id	13
Source ID	3

Low (Medium)

Password Autocomplete in Browser

Description	The AUTOCOMPLETE attribute is not disabled on an HTML FORM/INPUT element containing password type input. Passwords may be stored in browsers and retrieved.
URL	http://localhost:8000/admin/login/?next=/admin/
Method	GET
Parameter	id_password
Evidence	<input type="password" name="password" required id="id_password" />
URL	http://localhost:8000/admin
Method	GET
Parameter	id_password
Evidence	<input type="password" name="password" required id="id_password" />
Instances	2
Solution	Turn off the AUTOCOMPLETE attribute in forms or individual input elements containing password inputs by using AUTOCOMPLETE='OFF'.
Reference	http://www.w3schools.com/tags/att_input_autocomplete.asp
	https://msdn.microsoft.com/en-us/library/ms533486%28v=vs.85%29.aspx
CWE Id	525
WASC Id	15
Source ID	3