ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	5
Informational	3

Alert Detail

Medium (Medium)	X-Frame-Options Header Not Set	
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.	
	URL	http://www.securetx.com/index.html
	Method	GET
	Parameter	X-Frame-Options
	URL	http://www.securetx.com/
	Method	GET
	Parameter	X-Frame-Options
	URL	http://www.securetx.com/service.html
	Method	GET
	Parameter	X-Frame-Options
	URL	http://www.securetx.com/privacy.html
	Method	GET
	Parameter	X-Frame-Options
Instances	4	
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (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. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).	
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options	
CWE Id	16	
WASC Id	15	
Source ID	3	

Low (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	http://www.securetx.com/index.html
	Method	GET
	Evidence	<form id="contact-form" method="POST" action="http://fwme.land.com/securetxhome/sendmail/php/mail.php">
	URL	http://www.securetx.com/
	Method	GET
	Evidence	<form id="contact-form" method="POST" action="http://fwme.land.com/securetxhome/sendmail/php/mail.php">
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.	
Other Information	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret] was found in the following HTML form: [Form 1: "name" "email" "subject"].	
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery	
CWE Id	352	
WASC Id	9	
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://www.securetx.com/assets/img/icon1.png
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/assets/css/responsive.css
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/assets/img/partner-image.png
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/assets/img/logo.png
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/assets/js/jquery.min.js
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/assets/css/screenshot/screen-overview.css
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/index.html
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/assets/bootstrap-488.woff2
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/assets/fonts/semantic/semantic-consumer.min.css
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/assets/img/logo-three.png
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/assets/css/style.css
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/assets/img/favsy-idex.css
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/assets/img/scroll.min.css
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/service.html
	Method	GET
	Parameter	X-Content-Type-Options
	URL	http://www.securetx.com/assets/img/logotop-main.png
	Method	GET
	Parameter	X-Content-Type-Options
Instances	17	
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) if those pages are 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 scanner will not alert on client or server error responses.	
Reference	https://www.owasp.org/index.php/List_based_vulnerabilities/Missing_...........Content_Sniffing_Headers	
CWE Id	16	
WASC Id	15	
Source ID	3	

Low (Medium)	Private IP Disclosure	
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.	
	URL	http://www.securetx.com/plugins/plugins.min.js
	Method	GET
	Evidence	10.1.8.29
	URL	http://www.securetx.com/plugins/plugins.min.js
	Method	GET
	Evidence	10.74.76.92
Instances	2	
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP/PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.	
Other Information	10.1.8.29
	10.74.76.92
	10.9.1.1
	10.9.1.1
Reference	https://tools.ietf.org/html/rfc1918	
CWE Id	200	
WASC Id	13	
Source ID	3	

Informational (Medium)	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://www.securetx.com/index.html
	Method	GET
	URL	http://www.securetx.com/
	Method	GET
	URL	http://www.securetx.com/service.html
	Method	GET
Instances	3	
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.	
Other Information	The following comment/snippet was identified via the pattern: \bFROM\b
	<!-- img src="assets/img/logotop.png" alt="Download From Playstore">
	The following comment/snippet was identified via the pattern: \bFROM\b
	<!-- <li class="py-1">
	<a href="assets/img/logos.png" alt="Download From Playstore">
	<img ...
	The following comment/snippet was identified via the pattern: \bFROM\b
	<!-- Warrant from fwme.land.com/securetxhome/mail.htm p FTTrack Website Copyr3.+ (HT&CGCE/IA); Wed, 04 Feb 2020 09:19:11 GMT -->
Reference		
CWE Id	200	
WASC Id	13	
Source ID	3	

Informational (Low)	Timestamp Disclosure - Unix	
Description	A timestamp was disclosed by the application/web server - Unix	
	URL	http://www.securetx.com/favsindex_17_26.apk
	Method	GET
	Evidence	53384064
	URL	http://www.securetx.com/favsindex_17_26.apk
	Method	GET
	Evidence	0886672227
	URL	http://www.securetx.com/favsindex_17_26.apk
	Method	GET
	Evidence	80809000
	URL	http://www.securetx.com/favsindex_17_26.apk
	Method	GET
	Evidence	90867979
	URL	http://www.securetx.com/plugins/highchart/highcharter_security.jpg
	Method	GET
	Evidence	29844791
	URL	http://www.securetx.com/plugins/highchart/highcharter_security.jpg
	Method	GET
	Evidence	16033203
Instances	94	
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.	
Other Information	53384064, which evaluates to: 1971-08-29 00:34:44	
Reference	http://projects.webappsec.org/w/page/13246985/Information%20Leakage	
CWE Id	200	
WASC Id	13	
Source ID	3	

Informational (Low)	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://www.securetx.com/assets/js/bootstrap/bootstrap.min.js
	Method	GET
	URL	http://www.securetx.com/assets/jquery/jquery-2.3.1.min.js
	Method	GET
	URL	http://www.securetx.com/plugins/jscharts.js
	Method	GET
	URL	http://www.securetx.com/plugins/plugins.min.js
	Method	GET
Instances	4	
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.	
Other Information	The following comment/snippet was identified via the pattern: \bfrom\b
Reference		
CWE Id	200	
WASC Id	13	
Source ID	3	