ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	6
Informational	2

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://13.233.250.119/quality_standards
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/s?current_refinement=Experiences
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/help/article/17/who-can-host-on-site-name
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/help/topic/13/sign-up
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/help/article/8/welcome-your-guests
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/help/article/13/how-do-i-book-a-place-on-site-name
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/help/article/4/book
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/help/topic/3/how-to-host
Method	GET

Parameter	X-Frame-Options
URL	http://13.233.250.119/help
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/s?current_refinement=Homes
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/help/article/15/what-is-a-pre-approval
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/help/article/10/what-are-the-requirements-to-book-on-site-name
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/help/article/3/search
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/help/article/7/respond-to-requests
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/trust_safety
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/about_us
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/help/article/14/what-is-instant-book
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/guest_refund
Method	GET
Parameter	X-Frame-Options
URL	http://13.233.250.119/help/article/9/how-do-i-create-an-account
Method	GET
Parameter	X-Frame-Options

URL	http://13.233.250.119/help/topic/5/deciding-to-host
Method	GET
Parameter	X-Frame-Options
Instances	48
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
Medium (Medium)	**Application Error Disclosure**
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	http://13.233.250.119/js/host_experiences/host_experience.js?v=tqZcN
Method	GET
Evidence	Internal Server Error
Instances	1
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	200
WASC Id	13
Source ID	3
Medium (Medium)	**Directory Browsing**
Description	It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information.
URL	http://13.233.250.119/js/host_experiences/
Method	GET
Attack	Parent Directory
URL	http://13.233.250.119/images/host_experiences/
Method	GET
Attack	Parent Directory
URL	http://13.233.250.119/images/room_type/
Method	GET
Attack	Parent Directory
Instances	3
Solution	Disable directory browsing. If this is required, make sure the listed files does not induce risks.
Reference	http://httpd.apache.org/docs/mod/core.html#options http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html

CWE Id	548
WASC Id	48
Source ID	1
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://13.233.250.119/js/angular.js
Method	GET
Evidence	<form name="myForm" ng-controller="ExampleController">
URL	http://13.233.250.119/help/topic/9/finding-a-place
Method	GET
Evidence	<form method="POST" action="http://13.233.250.119/authenticate" accept-charset="UTF-8" novalidate="true" data-action="Signin">
URL	http://13.233.250.119/help/article/16/how-do-i-submit-a-reservation-request
Method	GET
Evidence	<form method="POST" action="http://13.233.250.119/authenticate" accept-charset="UTF-8" novalidate="true" data-action="Signin">
URL	http://13.233.250.119/help
Method	GET
Evidence	<form class="search-input-container" id="help-search-container">
URL	http://13.233.250.119/help/article/7/respond-to-requests
Method	GET
Evidence	<form class="search-input-container" id="help-search-container">
URL	http://13.233.250.119/help/topic/2/how-to-travel
Method	GET
Evidence	<form method="POST" action="http://13.233.250.119/forgot_password" accept-charset="UTF-8">
URL	http://13.233.250.119/help/topic/13/sign-up
Method	GET
Evidence	<form method="POST" action="http://13.233.250.119/authenticate" accept-charset="UTF-8" novalidate="true" data-action="Signin">

URL	http://13.233.250.119/contact
Method	GET
Evidence	<form method="POST" action="http://13.233.250.119/create" accept-charset="UTF-8" class="signup-form" data-action="Signup" id="user_new" novalidate="true">
URL	http://13.233.250.119/help/article/2/trusted-services
Method	GET
Evidence	<form method="POST" action="http://13.233.250.119/create" accept-charset="UTF-8" class="signup-form" data-action="Signup" id="user_new" novalidate="true">
URL	http://13.233.250.119/terms_of_service
Method	GET
Evidence	<form method="POST" action="http://13.233.250.119/forgot_password" accept-charset="UTF-8">
URL	http://13.233.250.119/help/article/18/what-are-the-quality-standards-for-experiences
Method	GET
Evidence	<form class="search-input-container" id="help-search-container">
URL	http://13.233.250.119/s
Method	GET
Evidence	<form class="wl-modal-form d-none">
URL	http://13.233.250.119/%7B%7Bexplore.search_url%7D%7D
Method	GET
Evidence	<form method="POST" action="http://13.233.250.119/create" accept-charset="UTF-8" class="signup-form" data-action="Signup" id="user_new" novalidate="true">
URL	http://13.233.250.119/help/article/3/search
Method	GET
Evidence	<form class="search-input-container" id="help-search-container">
URL	http://13.233.250.119/sitemap.xml
Method	GET
Evidence	<form action="http://13.233.250.119/s" class="search-form header_search_form">
URL	http://13.233.250.119/help/topic/16/quality-standards
Method	GET
Evidence	<form method="POST" action="http://13.233.250.119/authenticate" accept-charset="UTF-8" novalidate="true" data-action="Signin">
URL	http://13.233.250.119/js/angular.js
Method	GET
Evidence	<form name="userForm">
URL	http://13.233.250.119/copyright_policy
Method	GET
Evidence	<form action="http://13.233.250.119/s" class="search-form header_search_form">
URL	http://13.233.250.119/guest_refund
Method	GET
Evidence	<form method="POST" action="http://13.233.250.119/authenticate" accept-charset="UTF-8" novalidate="true" data-action="Signin">
URL	http://13.233.250.119/help/article/1/a-community-built-on-sharing
Method	GET

Evidence	<form method="POST" action="http://13.233.250.119/forgot_password" accept-charset="UTF-8">
Instances	267
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 14: "input"].
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
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://13.233.250.119/css/jquery-ui.css?v=OYKDb
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/css/common_ie8.css?v=S9pbT
Method	GET
Paramete	X-Content-Type-Options

r	
URL	http://13.233.250.119/js/me-lazyload.js
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/css/common_ie8.css?v=RspFT
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/css/common_ie8.css?v=LSWaQ
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/js/nouislider.min.js?v=p1BPR
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/js/jquery.textfill.min.js?v=QIZv6
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/css/common_ie8.css?v=i0Jji
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/js/jquery.selectBoxIt.js
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/help/article/6/list-your-space
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/js/nouislider.min.js?v=4OAni
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/js/common.js?v=MfxyQ
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/help/topic/3/how-to-host
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/js/nouislider.min.js?v=i0Jji

Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/js/jquery.textfill.min.js?v=S9pbT
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/js/common.js?v=i0Jji
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/css/common.css?v=w4mUD
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/s?current_refinement=Experiences
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/js/nouislider.min.js?v=QIZv6
Method	GET
Parameter	X-Content-Type-Options
URL	http://13.233.250.119/css/common_ie8.css?v=4OAni
Method	GET
Parameter	X-Content-Type-Options
Instances	469
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. At "High" threshold this scan rule will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	16
WASC Id	15
Source ID	3
Low (Medium)	**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	http://13.233.250.119/authenticate
Method	POST
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/s?current_refinement=Homes
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/help/topic/9/finding-a-place
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/help/article/14/what-is-instant-book
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/help/topic/13/sign-up
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/help/article/16/how-do-i-submit-a-reservation-request
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/%7B%7Bexplore.search_url%7D%7D
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/dashboard
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/%7B%7B%20host_experience.link%20%7D%7D
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/guest_refund
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/trips/current
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/privacy_policy
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/quality_standards
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/why_host
Method	GET
Evidence	X-Powered-By: PHP/7.3.23

URL	http://13.233.250.119/users/show/0
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/rooms/%7B%7Brooms.id%7D%7D?checkin=%7B%7Bcheckin%7D%7D&checkout=%7B%7Bcheckout%7D%7D&guests=%7B%7Bguests%7D%7D
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/help/article/2/trusted-services
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/signup_login
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/help/article/6/list-your-space
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
URL	http://13.233.250.119/help/topic/16/quality-standards
Method	GET
Evidence	X-Powered-By: PHP/7.3.23
Instances	71
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
Source ID	3

Low (Medium)	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	http://13.233.250.119/contact
Method	GET
Parameter	https://maps.googleapis.com/maps/api/js?key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en
Evidence	<script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en"></script>
URL	http://13.233.250.119/host_guarantee
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/socket.io/2.3.0/socket.io.dev.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/socket.io/2.3.0/socket.io.dev.js"></script>
URL	http://13.233.250.119/invite
	GET

Method	
Parameter	https://apis.google.com/js/api:client.js
Evidence	<script src="https://apis.google.com/js/api:client.js"></script>
URL	http://13.233.250.119/%7B%7Broom.link%7D%7D
Method	GET
Parameter	https://maps.googleapis.com/maps/api/js?key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en
Evidence	<script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en"></script>
URL	http://13.233.250.119/consent_disagree
Method	GET
Parameter	https://maps.googleapis.com/maps/api/js?key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en
Evidence	<script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en"></script>
URL	http://13.233.250.119/help/article/3/search
Method	GET
Parameter	https://maps.googleapis.com/maps/api/js?key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en
Evidence	<script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en"></script>
URL	http://13.233.250.119/login
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/socket.io/2.3.0/socket.io.dev.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/socket.io/2.3.0/socket.io.dev.js"></script>
URL	http://13.233.250.119/help/topic/1/how-it-works
Method	GET
Parameter	https://apis.google.com/js/api:client.js
Evidence	<script src="https://apis.google.com/js/api:client.js"></script>
URL	http://13.233.250.119/help/article/9/how-do-i-create-an-account
Method	GET
Parameter	https://apis.google.com/js/api:client.js
Evidence	<script src="https://apis.google.com/js/api:client.js"></script>
URL	http://13.233.250.119/help/topic/5/deciding-to-host
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/socket.io/2.3.0/socket.io.dev.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/socket.io/2.3.0/socket.io.dev.js"></script>
URL	http://13.233.250.119/help/article/5/travel
Method	GET
Parameter	https://maps.googleapis.com/maps/api/js?

r	key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en
Evidence	<script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en"></script>
URL	http://13.233.250.119/%7B%7B%20host_experience.link%20%7D%7D
Method	GET
Parameter	https://cdn.jsdelivr.net/qtip2/3.0.3/jquery.qtip.min.js
Evidence	<script type="text/javascript" src="https://cdn.jsdelivr.net/qtip2/3.0.3/jquery.qtip.min.js"></script>
URL	http://13.233.250.119/%7B%7Bour_community.link%7D%7D
Method	GET
Parameter	https://apis.google.com/js/api:client.js
Evidence	<script src="https://apis.google.com/js/api:client.js"></script>
URL	http://13.233.250.119/help/topic/16/quality-standards
Method	GET
Parameter	https://cdn.jsdelivr.net/qtip2/3.0.3/jquery.qtip.min.js
Evidence	<script type="text/javascript" src="https://cdn.jsdelivr.net/qtip2/3.0.3/jquery.qtip.min.js"></script>
URL	http://13.233.250.119/signup_login
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/socket.io/2.3.0/socket.io.dev.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/socket.io/2.3.0/socket.io.dev.js"></script>
URL	http://13.233.250.119/host/experiences
Method	GET
Parameter	https://apis.google.com/js/api:client.js
Evidence	<script src="https://apis.google.com/js/api:client.js"></script>
URL	http://13.233.250.119/help/topic/5/deciding-to-host
Method	GET
Parameter	https://apis.google.com/js/api:client.js
Evidence	<script src="https://apis.google.com/js/api:client.js"></script>
URL	http://13.233.250.119/trust_safety
Method	GET
Parameter	https://maps.googleapis.com/maps/api/js?key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en
Evidence	<script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en"></script>
URL	http://13.233.250.119/help/topic/13/sign-up
Method	GET
Parameter	https://cdn.jsdelivr.net/qtip2/3.0.3/jquery.qtip.min.js
Evidence	<script type="text/javascript" src="https://cdn.jsdelivr.net/qtip2/3.0.3/jquery.qtip.min.js"></script>
URL	http://13.233.250.119/help/article/18/what-are-the-quality-standards-for-experiences

Method	GET
Parameter	https://maps.googleapis.com/maps/api/js?key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en
Evidence	<script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyB6lCQnISdsSUVFdcQYxaHxXXjvKDn9wcs&libraries=places&language=en"></script>
Instances	232
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Source ID	3

Low (Medium)	**Cookie No HttpOnly Flag**
Description	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://13.233.250.119/sitemap.xml
Method	GET
Parameter	PHPSESSID
Evidence	Set-Cookie: PHPSESSID
URL	http://13.233.250.119/
Method	GET
Parameter	PHPSESSID
Evidence	Set-Cookie: PHPSESSID
Instances	2
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	16
WASC Id	13
Source ID	3

Low (Medium)	**Cookie Without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	http://13.233.250.119/sitemap.xml
Method	GET
Parameter	PHPSESSID
Evidence	Set-Cookie: PHPSESSID
URL	http://13.233.250.119/
Method	GET
Paramete	PHPSESSID

r	
Evidence	Set-Cookie: PHPSESSID
Instances	2
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	16
WASC Id	13
Source ID	3

Informational (Low)	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server - Unix
URL	http://13.233.250.119/help/article/13/how-do-i-book-a-place-on-site-name
Method	GET
Evidence	13184720
URL	http://13.233.250.119/css/common.css?v=QIZv6
Method	GET
Evidence	85714286
URL	http://13.233.250.119/css/common.css?v=gtGkY
Method	GET
Evidence	66666667
URL	http://13.233.250.119/css/common.css?v=RspFT
Method	GET
Evidence	00000059
URL	http://13.233.250.119/help/article/4/book
Method	GET
Evidence	13184720
URL	http://13.233.250.119/css/common.css?v=p1BPR
Method	GET
Evidence	00000059
URL	http://13.233.250.119/css/common.css?v=S9pbT
Method	GET
Evidence	00000059
URL	http://13.233.250.119/css/common.css?v=ZdjCN
Method	GET
Evidence	66666667
URL	http://13.233.250.119/css/common_ie8.css?v=IH4dU
Method	GET
Evidence	00000000
URL	http://13.233.250.119/css/common_ie8.css?v=p1BPR
Method	GET
Evidence	999999999
URL	http://13.233.250.119/css/common.css?v=YBwGu

Method	GET
Evidence	33333333
URL	http://13.233.250.119/css/common.css?v=LSWaQ
Method	GET
Evidence	00000059
URL	http://13.233.250.119/css/common.css?v=p1BPR
Method	GET
Evidence	85714286
URL	http://13.233.250.119/css/common.css?v=i0Jji
Method	GET
Evidence	00000059
URL	http://13.233.250.119/about_us
Method	GET
Evidence	13184720
URL	http://13.233.250.119/css/common.css?v=e96PI
Method	GET
Evidence	33333333
URL	http://13.233.250.119/css/common_ie8.css?v=S9pbT
Method	GET
Evidence	999999999
URL	http://13.233.250.119/css/common.css?v=fQhqH
Method	GET
Evidence	33333333
URL	http://13.233.250.119/css/common.css?v=S9pbT
Method	GET
Evidence	85714286
URL	http://13.233.250.119/help/article/8/welcome-your-guests
Method	GET
Evidence	13184720
Instances	428
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Other information	13184720, which evaluates to: 1970-06-02 19:55:20
Reference	http://projects.webappsec.org/w/page/13246936/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://13.233.250.119/why_host
Method	GET

URL	http://13.233.250.119/js/nouislider.min.js?v=fGZiE
Method	GET
URL	http://13.233.250.119/js/common.js?v=nUPio
Method	GET
URL	http://13.233.250.119/js/common.js?v=qKrg4
Method	GET
URL	http://13.233.250.119/help/article/15/what-is-a-pre-approval
Method	GET
URL	http://13.233.250.119/js/nouislider.min.js?v=w4mUD
Method	GET
URL	http://13.233.250.119/users/show/0
Method	GET
URL	http://13.233.250.119/js/inbox.js?v=IH4dU
Method	GET
URL	http://13.233.250.119/js/common.js?v=XUctG
Method	GET
URL	http://13.233.250.119/help/article/2/trusted-services
Method	GET
URL	http://13.233.250.119/js/host_experiences/owl.carousel.js?v=tqZcN
Method	GET
URL	http://13.233.250.119/privacy_policy
Method	GET
URL	http://13.233.250.119/js/search.js?v=QIZv6
Method	GET
URL	http://13.233.250.119/js/common.js?v=gj5ml
Method	GET
URL	http://13.233.250.119/js/inbox.js?v=mUfAM
Method	GET
URL	http://13.233.250.119/js/common.js?v=gLoKO
Method	GET
URL	http://13.233.250.119/host_guarantee
Method	GET
URL	http://13.233.250.119/js/common.js?v=mUfAM
Method	GET
URL	http://13.233.250.119/js/nouislider.min.js?v=2F3oc
Method	GET
URL	http://13.233.250.119/js/inbox.js?v=XUctG
Method	GET
Instances	243
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: \bSELECT\b

```
<script type="text/javascript">
$(document).ready(function() {
$('.top-home').click(function(event){
event.stopPropagation();
});
$(function() {
var selectBox = $("select.footer-select").selectBoxIt();
var selectBox2 = $("select.custom-select").selectBoxIt();
});
$('ul.menu-group li a').click(function() {
$('.nav--sm').css('visibility','hidden');
});
$('.burger--sm').click(function() {
$('.header--sm .nav--sm').css('visibility','visible');
$('.makent-header .header--sm .nav-content--sm').css('left','0', 'important');
});
$('.nav-mask--sm').click(function()
{
$('.header--sm .nav--sm').css('visibility','hidden');
$('.makent-header .header--sm .nav-content--sm').css('left','-285px');
});
$('.nav-mask--sm').click(function() {
$('.header--sm .nav--sm').css('visibility','hidden');
$('.makent-header .header--sm .nav-content--sm').css('left','-285px');
});
$(document).on('change','#user_profile_pic', function() {
$('#ajax_upload_form').submit();
});
});
</script>
```

Reference	
CWE Id	200
WASC Id	13
Source ID	3