ZAP Scanning Report

preliminary security scan - only basic PHP and MySQL pwd authentication methods

Sites: https://spocs.getpocket.com https://www.gstatic.com https://www.google.com https://cdn.jsdelivr.net http://13.215.200.46

Generated on Sun, 29 Oct 2023 17:02:51

ZAP Version: 2.14.0

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	8
Low	7
Informational	9

Alerts

Name	Risk Level	Number of Instances
SQL Injection - MySQL	High	1
Absence of Anti-CSRF Tokens	Medium	5
Application Error Disclosure	Medium	3
Content Security Policy (CSP) Header Not Set	Medium	25
Cross-Domain Misconfiguration	Medium	4
Directory Browsing	Medium	2
Hidden File Found	Medium	1
Missing Anti-clickjacking Header	Medium	17
Parameter Tampering	Medium	2
Cookie No HttpOnly Flag	Low	1
Cookie without SameSite Attribute	Low	1
Cross-Domain JavaScript Source File Inclusion	Low	7
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	38
Strict-Transport-Security Header Not Set	Low	2
Timestamp Disclosure - Unix	Low	18
X-Content-Type-Options Header Missing	Low	31
Authentication Request Identified	Informational	1
GET for POST	Informational	2
Information Disclosure - Suspicious Comments	Informational	19
Modern Web Application	Informational	6
Re-examine Cache-control Directives	Informational	1
Retrieved from Cache	Informational	35

Session Management Response Identified	Informational	14
User Agent Fuzzer	Informational	24
User Controllable HTML Element Attribute (Potential XSS)	Informational	2

Alert Detail

High	**SQL Injection - MySQL**
Description	SQL injection may be possible.
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east,central,east,west
Method	GET
Attack	north,north-east,central,east,west') UNION ALL select NULL --
Evidence	The used SELECT statements have a different number of columns
Other Info	RDBMS [MySQL] likely, given UNION-specific error message regular expression [\QThe used SELECT statements have a different number of columns\E] matched by the HTML results The vulnerability was detected by manipulating the parameter with an SQL UNION clause to cause a database error message to be returned and recognised
Instances	1
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40018

Medium	**Absence of Anti-CSRF Tokens**
	No Anti-CSRF tokens were found in a HTML submission form.

Description	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://13.215.200.46/pages/JoinAnEvent.php
Method	GET
Attack	
Evidence	<form class="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: "search"].
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	<form method="post" onsubmit="return validateForm()">
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: "password1" "username1"].
URL	http://13.215.200.46/pages/SignUp.php
Method	GET
Attack	
Evidence	<form method="post" onsubmit="return validateForm()">
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: "dob1" "email1" "name1" "password1" "password2" "username1"].
URL	http://13.215.200.46/pages/LogIn.php
Method	POST
Attack	
Evidence	<form method="post" onsubmit="return validateForm()">
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: "password1" "username1"].

URL	http://13.215.200.46/pages/SignUp.php
Method	POST
Attack	
Evidence	<form method="post" onsubmit="return validateForm()">
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: "dob1" "email1" "name1" "password1" "password2" "username1"].
Instances	5
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

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://13.215.200.46/pages/FindAGarden.php
Method	GET
Attack	

Evidence	<b>Warning</b>: Undefined array key "username" in <b>/var/www/html/pages/FindAGarden.php</b> on line <b>310</b><br />
Other Info	
URL	http://13.215.200.46/pages/Profile.php
Method	GET
Attack	
Evidence	<b>Warning</b>: Undefined array key "username" in <b>/var/www/html/pages/Profile.php</b> on line <b>150</b><br />
Other Info	
URL	http://13.215.200.46/pages/ProfileEdit.php
Method	GET
Attack	
Evidence	<b>Warning</b>: Undefined array key "username" in <b>/var/www/html/pages/ProfileEdit.php</b> on line <b>295</b><br />
Other Info	
Instances	3
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
Plugin Id	90022

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://13.215.200.46/favicon.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/FindAGarden.html
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/FindAGarden.php

Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/icons.png
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/JoinAnEvent.html
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/JoinAnEvent.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/LandingPage.html
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/logo.png
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=central
Method	GET
Attack	

Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=east
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=east,west
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east,central
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east,central,east
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east,central,east,west
Method	GET
Attack	
Evidence	

Other Info	
URL	http://13.215.200.46/pages/Profile.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/ProfileEdit.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/public/images/search.svg
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/SignUp.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/LogIn.php
Method	POST
Attack	
Evidence	
Other Info	

URL	http://13.215.200.46/pages/SignUp.php
Method	POST
Attack	
Evidence	
Other Info	
Instances	25
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.1/dist/css/bootstrap.min.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.1/dist/js/bootstrap.bundle.min.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/js/bootstrap.bundle.min.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser

Other Info	implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	4
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Medium	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://13.215.200.46/pages/
Method	GET
Attack	http://13.215.200.46/pages/
Evidence	Parent Directory
Other Info	
URL	http://13.215.200.46/pages/MySQL/
Method	GET
Attack	http://13.215.200.46/pages/MySQL/
Evidence	Parent Directory
Other Info	
Instances	2
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
Plugin Id	0

Medium	Hidden File Found
Description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	http://13.215.200.46/.DS_Store
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	ds_store
Instances	1
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
CWE Id	538
WASC Id	13
Plugin Id	40035

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://13.215.200.46/pages/FindAGarden.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/JoinAnEvent.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/LandingPage.html
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	
Other	

Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=central
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=east
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=east,west
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east,central
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east,central,east
Method	GET
Attack	
Evidence	
Other Info	
	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east,central,east,

URL	west
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/Profile.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/ProfileEdit.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/SignUp.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/LogIn.php
Method	POST
Attack	
Evidence	
Other Info	
URL	http://13.215.200.46/pages/SignUp.php
Method	POST
Attack	
Evidence	
Other Info	
Instances	17
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021

WASC Id	15
Plugin Id	10020

Medium	Parameter Tampering
Description	Parameter manipulation caused an error page or Java stack trace to be displayed. This indicated lack of exception handling and potential areas for further exploit.
URL	http://13.215.200.46/pages/MySQL/Event.php?=&regions=north%2Cnorth-east%2Ccentral%2Ceast%2Cwest
Method	GET
Attack	
Evidence	on line <b>
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&=
Method	GET
Attack	
Evidence	on line <b>
Other Info	
Instances	2
Solution	Identify the cause of the error and fix it. Do not trust client side input and enforce a tight check in the server side. Besides, catch the exception properly. Use a generic 500 error page for internal server error.
Reference	
CWE Id	472
WASC Id	20
Plugin Id	40008

Low	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://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
Instances	1
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	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://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
Instances	1
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	[1275](1275)
WASC Id	13
Plugin Id	[10054](10054)

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	http://13.215.200.46/pages/FindAGarden.php
Method	GET
Attack	
Evidence	<script src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBlsN7cu3WF-W3FGrtJ7l9El4nKPAyN1r8&map_ids=40c99f5bd3e0f892&callback=initMap"></script>
Other Info	
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	<script src="https://unpkg.com/vue@next"></script>
Other Info	
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	<script src="https://www.google.com/recaptcha/api.js" async defer></script>
Other Info	
URL	http://13.215.200.46/pages/SignUp.php
Method	GET
Attack	
Evidence	<script src="https://unpkg.com/vue@next"></script>
Other Info	
URL	http://13.215.200.46/pages/LogIn.php
Method	POST

Attack	
Evidence	<script src="https://unpkg.com/vue@next"></script>
Other Info	
URL	http://13.215.200.46/pages/LogIn.php
Method	POST
Attack	
Evidence	<script src="https://www.google.com/recaptcha/api.js" async defer></script>
Other Info	
URL	http://13.215.200.46/pages/SignUp.php
Method	POST
Attack	
Evidence	<script src="https://unpkg.com/vue@next"></script>
Other Info	
Instances	7
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
Plugin Id	10017

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://13.215.200.46/favicon.ico
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/icons.png
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/logo.png
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	

URL	http://13.215.200.46/pages/FindAGarden.html
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/FindAGarden.php
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/icons.png
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/JoinAnEvent.html
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/JoinAnEvent.php
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/LandingPage.html
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/logo.png

Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=central
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=east
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=east,west
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east,central
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east,central,east
Method	GET
Attack	

Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east,central,east,west
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/Profile.php
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/ProfileEdit.php
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/public/images/search.svg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/SignUp.php
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/public/images/calendar.svg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/public/images/defaultProfile.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)

Other Info	
URL	http://13.215.200.46/public/images/edit.png
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/public/images/EventImage.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/public/images/instagram.png
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/public/images/linkedin.png
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/public/images/location%20pin.svg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/public/images/logout.png
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/public/images/open-mail.png
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	

URL	http://13.215.200.46/public/images/telegram.png
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/robots.txt
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/sitemap.xml
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/style.css
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/LogIn.php
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://13.215.200.46/pages/SignUp.php
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
Instances	38
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13

Plugin Id	10036

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://www.google.com/recaptcha/api.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	
Other Info	
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1396182291
Other Info	1396182291, which evaluates to: 2014-03-30 20:24:51
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1426881987
Other Info	1426881987, which evaluates to: 2015-03-21 04:06:27
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET

Attack	
Evidence	1508970993
Other Info	1508970993, which evaluates to: 2017-10-26 06:36:33
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1518500249
Other Info	1518500249, which evaluates to: 2018-02-13 13:37:29
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1537002063
Other Info	1537002063, which evaluates to: 2018-09-15 17:01:03
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1541459225
Other Info	1541459225, which evaluates to: 2018-11-06 07:07:05
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1555081692
Other Info	1555081692, which evaluates to: 2019-04-12 23:08:12
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1695183700
Other Info	1695183700, which evaluates to: 2023-09-20 12:21:40
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-26 09:23:13
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	

Evidence	1747873779
Other Info	1747873779, which evaluates to: 2025-05-22 08:29:39
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1779033703
Other Info	1779033703, which evaluates to: 2026-05-18 00:01:43
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1859775393
Other Info	1859775393, which evaluates to: 2028-12-07 12:16:33
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1899447441
Other Info	1899447441, which evaluates to: 2030-03-11 16:17:21
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1925078388
Other Info	1925078388, which evaluates to: 2031-01-02 07:59:48
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1955562222
Other Info	1955562222, which evaluates to: 2031-12-21 03:43:42
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1986661051
Other Info	1986661051, which evaluates to: 2032-12-15 02:17:31
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	1996064986
Other	

Other Info	1996064986, which evaluates to: 2033-04-02 22:29:46
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	2000000000
Other Info	2000000000, which evaluates to: 2033-05-18 11:33:20
Instances	18
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Plugin Id	10096

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://13.215.200.46/icons.png
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://13.215.200.46/logo.png
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://13.215.200.46/pages/FindAGarden.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://13.215.200.46/pages/JoinAnEvent.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://13.215.200.46/pages/LandingPage.html
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://13.215.200.46/pages/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://13.215.200.46/pages/MySQL/Event.php?key=&regions=central
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://13.215.200.46/pages/MySQL/Event.php?key=&regions=east
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://13.215.200.46/pages/MySQL/Event.php?key=&regions=east,west
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://13.215.200.46/pages/MySQL/Event.php?key=&regions=north
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://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east
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://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east,central
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://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east,central,east
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://13.215.200.46/pages/MySQL/Event.php?key=&regions=north,north-east,central,east,west
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://13.215.200.46/pages/Profile.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://13.215.200.46/pages/ProfileEdit.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://13.215.200.46/pages/SignUp.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://13.215.200.46/public/images/calendar.svg
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://13.215.200.46/public/images/defaultProfile.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://13.215.200.46/public/images/edit.png
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://13.215.200.46/public/images/EventImage.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://13.215.200.46/public/images/instagram.png
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://13.215.200.46/public/images/linkedin.png
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://13.215.200.46/public/images/location%20pin.svg
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://13.215.200.46/public/images/logout.png
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://13.215.200.46/public/images/open-mail.png
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://13.215.200.46/public/images/telegram.png
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://13.215.200.46/style.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://13.215.200.46/pages/LogIn.php
Method	POST
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://13.215.200.46/pages/SignUp.php
Method	POST
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	https://spocs.getpocket.com/spocs
Method	POST
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	31
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Authentication Request Identified**
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	http://13.215.200.46/pages/LogIn.php
Method	POST
Attack	
Evidence	password1
Other	userParam=username1 userValue= passwordParam=password1 referer=http://13.

Info	215.200.46/pages/LogIn.php
Instances	1
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/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	GET for POST
Description	A request that was originally observed as a POST was also accepted as a GET. This issue does not represent a security weakness unto itself, however, it may facilitate simplification of other attacks. For example if the original POST is subject to Cross-Site Scripting (XSS), then this finding may indicate that a simplified (GET based) XSS may also be possible.
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	GET http://13.215.200.46/pages/LogIn.php?password1=ZAP&username1= HTTP/1.1
Other Info	
URL	http://13.215.200.46/pages/SignUp.php
Method	GET
Attack	
Evidence	GET http://13.215.200.46/pages/SignUp.php?dob1=2023-10-29&email1=ZAP&gender1=Gender&name1=&password1=ZAP&password2=ZAP&username1= HTTP/1.1
Other Info	
Instances	2
Solution	Ensure that only POST is accepted where POST is expected.
Reference	
CWE Id	16
WASC Id	20
Plugin Id	10058

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://13.215.200.46/pages/FindAGarden.php
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "<script> var mapLocation = {"garden":[{"gardenID":194,"gardenName":"[AHTC] BRP Bonsai Garden (Fish ball Noodle - Fo", see evidence field for the suspicious comment /snippet.
URL	http://13.215.200.46/pages/FindAGarden.php
Method	GET
Attack	

Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> function showGardenList(obj) { var output = ""; document.getElementById ("resultCount").i", see evidence field for the suspicious comment/snippet.
URL	http://13.215.200.46/pages/JoinAnEvent.php
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> function filter() { const checkboxes = document.querySelectorAll('input[type="checkbox"]:checked'", see evidence field for the suspicious comment/snippet.
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> const appUsername = Vue.createApp({ data(){ return {username1: ""}", see evidence field for the suspicious comment/snippet.
URL	http://13.215.200.46/pages/Profile.php
Method	GET
Attack	
Evidence	User
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script> var username = <br /> <b>Warning</b>: Undefined array key "username" in <b> /var/www/html/pages/Profile.ph", see evidence field for the suspicious comment/snippet.
URL	http://13.215.200.46/pages/Profile.php
Method	GET
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected in the element starting with: "<script> // idk if yall wanna try, but i wanted to add a button where when you click on the email, it copies onto yo", see evidence field for the suspicious comment/snippet.
URL	http://13.215.200.46/pages/ProfileEdit.php
Method	GET
Attack	
Evidence	User
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script> var username = <br /> <b>Warning</b>: Undefined array key "username" in <b> /var/www/html/pages/ProfileEdi", see evidence field for the suspicious comment/snippet.
URL	http://13.215.200.46/pages/SignUp.php
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> const appUsername = Vue.createApp({ data(){ ", see evidence field for the suspicious comment/snippet.
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.1/dist/js/bootstrap.bundle.min.js

Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():" function"==typeof define&&define.amd?def", see evidence field for the suspicious comment /snippet.
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/js/bootstrap.bundle.min.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():" function"==typeof define&&define.amd?def", see evidence field for the suspicious comment /snippet.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	dB
Other Info	The following pattern was used: \bDB\b and was detected 6 times, the first in the element starting with: "void 0,void 0),z|9)&&(z-6&E[1])<E[2])a:{for(l=c;l<window[E[0]].count;l++)if(X [13](32).contains(window[E[0]].clients[l].dB)){n=l;", see evidence field for the suspicious comment/snippet.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 14 times, the first in the element starting with: "t[6](20).test(n[O].src)){f=O;break a}f=-1}if((z|56)==z){for(N=l,d=[],G= ["cannot access the buffer of decoders over immutable dat", see evidence field for the suspicious comment/snippet.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: """ tabIndex="0">'],l='<div><div class="'+X[40](43,"rc-doscaptcha-header")+'"><div class="'+X[40](42,"rc-doscaptcha-header-text")", see evidence field for the suspicious comment/snippet.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 2 times, the first in the element starting with: "w}return(z|6)>>4||(l=V[23](47,this),O=g[4](E[2],this)+"",w=0,1<c&& (w=g[4](3,this)),this.S[l]=g[13](19,0,O,w)),n},function(z,c,l,", see evidence field for the suspicious comment/snippet.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js

Method	GET
Attack	
Evidence	Select
Other Info	The following pattern was used: \bSELECT\b and was detected 29 times, the first in the element starting with: "c),(z|16)==z&&(oG.call(this,c.eJ),this.type="action"),15))&&14>((z^10)&15))T[E[0]](22,function(H,x){T[20](8,this,x,H)},c,l);retu", see evidence field for the suspicious comment/snippet.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 6 times, the first in the element starting with: "l[1],this),r[34](64,l[U[0]],"vm_YDiq1BiI3a8zfbIPZjtF2",c),w=r[6](39,l[U[0]]),r[34](65,1,w,c),this.I=c[U[1]]()),1)<z&&(z+5^26)>=z", see evidence field for the suspicious comment/snippet.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 2 times, the first in the element starting with: "var Jw=new Ou("origin",Ya,"co"),Po=new Ou("size",(g[24](72,60,function(z,c,l,w,O,n,E,B){for(n=(O=(E=(c=K[7]((B=[26,0,"g"],4),c,B", see evidence field for the suspicious comment/snippet.
URL	http://13.215.200.46/pages/LogIn.php
Method	POST
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> const appUsername = Vue.createApp({ data(){ return {username1: ""}", see evidence field for the suspicious comment/snippet.
URL	http://13.215.200.46/pages/SignUp.php
Method	POST
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> const appUsername = Vue.createApp({ data(){ ", see evidence field for the suspicious comment/snippet.
Instances	19
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://13.215.200.46/pages/LandingPage.html
Method	GET
Attack	
Evidence	<a class="nav-link mx-2 disabled" href="#"><i class="about"></i> About</a>
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://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	<a class="nav-link mx-2 disabled" href="#"><i class="about"></i> About</a>
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://13.215.200.46/pages/Profile.php
Method	GET
Attack	
Evidence	<a href="#"> <button type="button" class=" btn bg-dark text-white mx-2"> <img src="../public/images/linkedin.png" class="editProfileimg"> LinkedIn </button> </a>
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://13.215.200.46/pages/SignUp.php
Method	GET
Attack	
Evidence	<a class="nav-link mx-2 disabled" href="#"><i class="about"></i> About</a>
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://13.215.200.46/pages/LogIn.php
Method	POST
Attack	
Evidence	<a class="nav-link mx-2 disabled" href="#"><i class="about"></i> About</a>
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://13.215.200.46/pages/SignUp.php
Method	POST
Attack	
Evidence	<a class="nav-link mx-2 disabled" href="#"><i class="about"></i> About</a>
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	6
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Re-examine Cache-control Directives**

Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://spocs.getpocket.com/spocs
Method	POST
Attack	
Evidence	
Other Info	
Instances	1
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	**Retrieved from Cache**
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.1/dist/css/bootstrap.min.css
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.1/dist/js/bootstrap.bundle.min.js
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/js/bootstrap.bundle.min.js
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js

Method	GET
Attack	
Evidence	Age: 13998
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1Bil3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14005
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1Bil3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14013
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1Bil3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14035
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1Bil3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14043
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1Bil3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14055
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1Bil3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14066
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1Bil3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	

Evidence	Age: 14069
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14074
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14083
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14084
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14088
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14089
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14097
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14098

Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14100
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14101
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14106
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14107
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14108
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14109
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14115
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.

URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14116
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14119
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14120
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14121
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14123
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14124
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14126
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET

Attack	
Evidence	Age: 14127
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14129
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/vm_YDiq1BiI3a8zfbIPZjtF2/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 14130
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
Instances	35
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
CWE Id	
WASC Id	
Plugin Id	10050

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://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	02be61svb42kvq0tfqcuitbm7s
Other Info	cookie:PHPSESSID
URL	http://13.215.200.46/pages/LogIn.php

Method	GET
Attack	
Evidence	1eq8afr9ebg8jj9bu3eq5her1r
Other Info	cookie:PHPSESSID
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	9rhkra1mhd1stlmd4phk2pqn8g
Other Info	cookie:PHPSESSID
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	ak9chp00756hv8ohgn6rlcq9td
Other Info	cookie:PHPSESSID
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	cs0rnlsjhk68q1agc1ufivfrr7
Other Info	cookie:PHPSESSID
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	ii4ud4djt0pbdtr5kqe1n5k6oo
Other Info	cookie:PHPSESSID
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	j3t7jl0t3pmake0ngnf6dqjhlc
Other Info	cookie:PHPSESSID
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	lcaaubmbh956o16tovmfns0sbb
Other Info	cookie:PHPSESSID
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	

Evidence	oo0ce2ob4ofjq7adi5ltn1kopi
Other Info	cookie:PHPSESSID
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	ul24ceee25tf58h1me72kd2np3
Other Info	cookie:PHPSESSID
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	9rhkra1mhd1stlmd4phk2pqn8g
Other Info	cookie:PHPSESSID
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	cs0rnlsjhk68q1agc1ufivfrr7
Other Info	cookie:PHPSESSID
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	ii4ud4djt0pbdtr5kqe1n5k6oo
Other Info	cookie:PHPSESSID
URL	http://13.215.200.46/pages/LogIn.php
Method	GET
Attack	
Evidence	j3t7jl0t3pmake0ngnf6dqjhlc
Other Info	cookie:PHPSESSID
Instances	14
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://13.215.200.46/pages

Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://13.215.200.46/pages
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://13.215.200.46/pages
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://13.215.200.46/pages
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://13.215.200.46/pages
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://13.215.200.46/pages
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://13.215.200.46/pages
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://13.215.200.46/pages
Method	GET

Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://13.215.200.46/pages
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://13.215.200.46/pages
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://13.215.200.46/pages
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://13.215.200.46/pages
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL
Method	GET

Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL
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://13.215.200.46/pages/MySQL
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://13.215.200.46/pages/MySQL
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://13.215.200.46/pages/MySQL
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL
Method	GET
	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML,

Attack	like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://13.215.200.46/pages/MySQL
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://13.215.200.46/pages/MySQL
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	24
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	[10104](10104)

Informational	**User Controllable HTML Element Attribute (Potential XSS)**
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	http://13.215.200.46/pages/SignUp.php
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://13.215.200.46/pages/SignUp.php appears to include user input in: a(n) [select] tag [id] attribute The user input found was: gender1=Gender The user-controlled value was: gender1
URL	http://13.215.200.46/pages/SignUp.php
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://13.215.200.46/pages/SignUp.php appears to include user input in: a(n) [select] tag [name] attribute The user input found was: gender1=Gender The user-controlled value was: gender1
Instances	2
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute

CWE Id	20
WASC Id	20
Plugin Id	10031