Web Application Vulnerability

Site: http://zero.webappsecurity.com

Generated on Tue, 10 Jun 2025 17:04:14

ZAP Version: 2.16.1

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	6
Low	3
Informational	4

Alerts

Name	Risk Level	Number of Instances
SQL Injection - SQLite	High	6
Absence of Anti-CSRF Tokens	Medium	3
Content Security Policy (CSP) Header Not Set	Medium	12
Cross-Domain Misconfiguration	Medium	25
Hidden File Found	Medium	1
Missing Anti-clickjacking Header	Medium	9
Vulnerable JS Library	Medium	2
Cookie without SameSite Attribute	Low	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	25
X-Content-Type-Options Header Missing	Low	21
Authentication Request Identified	Informational	3
Information Disclosure - Suspicious Comments	Informational	2
Modern Web Application	Informational	3
User Agent Fuzzer	Informational	96

Alert Detail

High	SQL Injection - SQLite
Description	SQL injection may be possible.
URL	http://zero.webappsecurity.com/resources/font/fontawesome-webfont.woff?v=3.0.1
Method	GET
Attack	case randomblob(10000000) when not null then 1 else 1 end
	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [422] milliseconds, parameter

Evidence	value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1,498] milliseconds, when the original unmodified query with value [3.0.1] took [484] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [422] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1,498] milliseconds, when the original unmodified query with value [3.0.1] took [484] milliseconds.
URL	http://zero.webappsecurity.com/search.html?searchTerm=ZAP
Method	GET
Attack	case randomblob(100000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1,213] milliseconds, parameter value [case randomblob(1000000000) when not null then 1 else 1 end], which caused the request to take [1,622] milliseconds, when the original unmodified query with value [ZAP] took [1,183] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1,213] milliseconds, parameter value [case randomblob(1000000000) when not null then 1 else 1 end], which caused the request to take [1,622] milliseconds, when the original unmodified query with value [ZAP] took [1,183] milliseconds.
URL	http://zero.webappsecurity.com/forgotten-password-send.html
Method	POST
Attack	case randomblob(1000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1,305] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1,611] milliseconds, when the original unmodified query with value [peBYbZrA] took [1,102] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1,305] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1,611] milliseconds, when the original unmodified query with value [peBYbZrA] took [1,102] milliseconds.
URL	http://zero.webappsecurity.com/signin.html
Method	POST
Attack	case randomblob(1000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [750] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1,120] milliseconds, when the original unmodified query with value [Sign in] took [355] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [750] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1,120] milliseconds, when the original unmodified query with value [Sign in] took [355] milliseconds.
URL	http://zero.webappsecurity.com/signin.html
Method	POST
Attack	case randomblob(1000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [904] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1,987] milliseconds, when the original unmodified query with value [JbJcAccMpLwmSXfG] took [346] milliseconds.

Other Info	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [904] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1,987] milliseconds, when the original unmodified query with value [JbJcAccMpLwmSXfG] took [346] milliseconds.
URL	http://zero.webappsecurity.com/signin.html
Method	POST
Attack	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [771] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [936] milliseconds, when the original unmodified query with value [] took [363] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [771] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [936] milliseconds, when the original unmodified query with value [] took [363] milliseconds.
Instances	6
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	40024

Medium	**Absence of Anti-CSRF Tokens**
	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL /form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a

Description	user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://zero.webappsecurity.com/forgot-password.html
Method	GET
Attack	
Evidence	<form id="send_password_form" action="/forgotten-password-send.html" method="post" class="form-horizontal">
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, _csrfToken] was found in the following HTML form: [Form 1: "submit" "user_email"].
URL	http://zero.webappsecurity.com/login.html
Method	GET
Attack	
Evidence	<form id="login_form" action="/signin.html" method="post" class="form-horizontal">
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, _csrfToken] was found in the following HTML form: [Form 1: "submit" "user_login" "user_password" "user_remember_me"].
URL	http://zero.webappsecurity.com/login.html?login_error=true
Method	GET
Attack	
Evidence	<form id="login_form" action="/signin.html" method="post" class="form-horizontal">
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, _csrfToken] was found in the following HTML form: [Form 1: "submit" "user_login" "user_password" "user_remember_me"].
Instances	3
	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Solution	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	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	**Content Security Policy (CSP) Header Not Set**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://zero.webappsecurity.com
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/favicon.ico
Method	GET
Attack	
Evidence	

Other Info	
URL	http://zero.webappsecurity.com/forgot-password.html
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/index.html
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/login.html
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/login.html?login_error=true
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/online-banking.html
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/search.html?searchTerm=ZAP
Method	GET
Attack	
Evidence	
Other Info	

URL	http://zero.webappsecurity.com/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/forgotten-password-send.html
Method	POST
Attack	
Evidence	
Other Info	
Instances	12
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**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	http://zero.webappsecurity.com
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	http://zero.webappsecurity.com/
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	http://zero.webappsecurity.com/favicon.ico
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	http://zero.webappsecurity.com/forgot-password.html
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	http://zero.webappsecurity.com/index.html
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	http://zero.webappsecurity.com/login.html
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	http://zero.webappsecurity.com/login.html?login_error=true
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	http://zero.webappsecurity.com/online-banking.html

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	http://zero.webappsecurity.com/resources/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	http://zero.webappsecurity.com/resources/css/font-awesome.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	http://zero.webappsecurity.com/resources/css/main.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	http://zero.webappsecurity.com/resources/font/fontawesome-webfont.woff?v=3.0.1
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	http://zero.webappsecurity.com/resources/img/main_carousel_1.jpg
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	http://zero.webappsecurity.com/resources/img/main_carousel_2.jpg
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	http://zero.webappsecurity.com/resources/img/main_carousel_3.jpg
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	http://zero.webappsecurity.com/resources/img/online_banking_hero.jpg
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	http://zero.webappsecurity.com/resources/js/bootstrap.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	http://zero.webappsecurity.com/resources/js/jquery-1.7.2.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	http://zero.webappsecurity.com/resources/js/jquery-1.8.2.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	http://zero.webappsecurity.com/resources/js/placeholders.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	http://zero.webappsecurity.com/robots.txt
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	http://zero.webappsecurity.com/search.html?searchTerm=ZAP
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	http://zero.webappsecurity.com/sitemap.xml
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	http://zero.webappsecurity.com/forgotten-password-send.html
Method	POST
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	http://zero.webappsecurity.com/signin.html
Method	POST
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	25
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	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://zero.webappsecurity.com/server-status
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	apache_server_status
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 https://httpd.apache.org/docs/current/mod/mod_status.html
CWE Id	538
WASC Id	13
Plugin Id	40035

Medium	Missing Anti-clickjacking Header
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	http://zero.webappsecurity.com
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/forgot-password.html
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/index.html
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/login.html
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/login.html?login_error=true
Method	GET
Attack	
Evidence	
Other	

Info	
URL	http://zero.webappsecurity.com/online-banking.html
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/search.html?searchTerm=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/forgotten-password-send.html
Method	POST
Attack	
Evidence	
Other Info	
Instances	9
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	**Vulnerable JS Library**
Description	The identified library appears to be vulnerable.
URL	http://zero.webappsecurity.com/resources/js/jquery-1.7.2.min.js
Method	GET
Attack	
Evidence	jquery-1.7.2.min.js
Other Info	The identified library jquery, version 1.7.2 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://github.com/jquery/jquery/issues/2432 http://research.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/jquery/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://bugs.jquery.com/ticket/11290 https://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

URL	http://zero.webappsecurity.com/resources/js/jquery-1.8.2.min.js
Method	GET
Attack	
Evidence	jquery-1.8.2.min.js
Other Info	The identified library jquery, version 1.8.2 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://github.com/jquery/jquery/issues/2432 http://research.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/jquery/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://bugs.jquery.com/ticket/11290 https://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
Instances	2
Solution	Upgrade to the latest version of the affected library.
Reference	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
CWE Id	1395
WASC Id	
Plugin Id	10003

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://zero.webappsecurity.com/signin.html
Method	POST
Attack	
Evidence	Set-Cookie: JSESSIONID
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
WASC Id	13
Plugin Id	10054

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://zero.webappsecurity.com
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	

URL	http://zero.webappsecurity.com/
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/favicon.ico
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/forgot-password.html
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/index.html
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/login.html
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/login.html?login_error=true
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/online-banking.html
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/resources/css/bootstrap.min.css
Method	GET

Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/resources/css/font-awesome.css
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/resources/css/main.css
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/resources/font/fontawesome-webfont.woff?v=3.0.1
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/resources/img/main_carousel_1.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/resources/img/main_carousel_2.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/resources/img/main_carousel_3.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/resources/img/online_banking_hero.jpg
Method	GET
Attack	

Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/resources/js/bootstrap.min.js
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/resources/js/jquery-1.7.2.min.js
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/resources/js/jquery-1.8.2.min.js
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/resources/js/placeholders.min.js
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/robots.txt
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/search.html?searchTerm=ZAP
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/sitemap.xml
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other	

Info	
URL	http://zero.webappsecurity.com/forgotten-password-send.html
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	http://zero.webappsecurity.com/signin.html
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
Instances	25
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10036

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://zero.webappsecurity.com
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://zero.webappsecurity.com/
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://zero.webappsecurity.com/forgot-password.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://zero.webappsecurity.com/index.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://zero.webappsecurity.com/login.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://zero.webappsecurity.com/login.html?login_error=true
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://zero.webappsecurity.com/online-banking.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://zero.webappsecurity.com/resources/css/bootstrap.min.css
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://zero.webappsecurity.com/resources/css/font-awesome.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://zero.webappsecurity.com/resources/css/main.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://zero.webappsecurity.com/resources/font/fontawesome-webfont.woff?v=3.0.1
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://zero.webappsecurity.com/resources/img/main_carousel_1.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://zero.webappsecurity.com/resources/img/main_carousel_2.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://zero.webappsecurity.com/resources/img/main_carousel_3.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://zero.webappsecurity.com/resources/img/online_banking_hero.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://zero.webappsecurity.com/resources/js/bootstrap.min.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://zero.webappsecurity.com/resources/js/jquery-1.7.2.min.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://zero.webappsecurity.com/resources/js/jquery-1.8.2.min.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://zero.webappsecurity.com/resources/js/placeholders.min.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://zero.webappsecurity.com/search.html?searchTerm=ZAP
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://zero.webappsecurity.com/forgotten-password-send.html
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	21
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	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://zero.webappsecurity.com/signin.html
Method	POST
Attack	
Evidence	user_password

Other Info	userParam=user_login userValue=ewxcUuOy passwordParam=user_password
	referer=http://zero.webappsecurity.com/login.html?login_error=true

URL	http://zero.webappsecurity.com/signin.html
Method	POST
Attack	
Evidence	user_password

Other Info	userParam=user_login userValue=JbJcAccMpLwmSXfG passwordParam=user_password
	referer=http://zero.webappsecurity.com/login.html?login_error=true

URL	http://zero.webappsecurity.com/signin.html
Method	POST
Attack	
Evidence	user_password

Other Info	userParam=user_login userValue=MkhfcCVr passwordParam=user_password
	referer=http://zero.webappsecurity.com/login.html

Instances	3
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	Information Disclosure - Suspicious Comments

Description	The response appears to contain suspicious comments which may help an attacker.
URL	http://zero.webappsecurity.com/resources/js/jquery-1.7.2.min.js
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//, bL=/\?/,bM=/<script\b[^<]*(?:(?!<\/script>)<[^<]*)*<\/script>/gi,bN=/^(?:select|textarea)/i,bO=/\s+/,bP=/([?&])_=[^&]*/,bQ=/^", see evidence field for the suspicious comment/snippet.
URL	http://zero.webappsecurity.com/resources/js/jquery-1.8.2.min.js
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//, cq=/\?/,cr=/<script\b[^<]*(?:(?!<\/script>)<[^<]*)*<\/script>/gi,cs=/([?&])_=[^&]*/,ct=/^([\w\+\.\-]+:)(?:\/\/([^\/?#:]*)(?::", see evidence field for the suspicious comment/snippet.
Instances	2
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
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://zero.webappsecurity.com
Method	GET
Attack	
Evidence	<a id="online-banking" class="btn btn-small btn-info">More Services</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://zero.webappsecurity.com/
Method	GET
Attack	
Evidence	<a id="online-banking" class="btn btn-small btn-info">More Services</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://zero.webappsecurity.com/index.html
Method	GET
Attack	
Evidence	<a id="online-banking" class="btn btn-small btn-info">More Services</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	3
Solution	This is an informational alert and so no changes are required.

Reference	
CWE Id	
WASC Id	
Plugin Id	10109

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

Info	
URL	http://zero.webappsecurity.com/login.html?login_error=true
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/login.html?login_error=true
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/login.html?login_error=true
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/login.html?login_error=true
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://zero.webappsecurity.com/login.html?login_error=true
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://zero.webappsecurity.com/login.html?login_error=true
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://zero.webappsecurity.com/login.html?login_error=true
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	

URL	http://zero.webappsecurity.com/login.html?login_error=true
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/login.html?login_error=true
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://zero.webappsecurity.com/login.html?login_error=true
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://zero.webappsecurity.com/login.html?login_error=true
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	

URL	http://zero.webappsecurity.com/resources
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources
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://zero.webappsecurity.com/resources
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://zero.webappsecurity.com/resources
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://zero.webappsecurity.com/resources
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources
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://zero.webappsecurity.com/resources
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://zero.webappsecurity.com/resources
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/css
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/css
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/css

Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/css
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/css
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/css
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/css
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/css
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/css
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/font

Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/font
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/font
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/font
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/font
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://zero.webappsecurity.com/resources/font
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://zero.webappsecurity.com/resources/font
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://zero.webappsecurity.com/resources/font
Method	GET

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

Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/img
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/img
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/img
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/img
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/img
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/img
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/img
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://zero.webappsecurity.com/resources/img
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/img
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0

Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/js
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/js
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/js
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/js
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/resources/js
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)

Evidence	
Other Info	
URL	http://zero.webappsecurity.com/signin.html
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/signin.html
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/signin.html
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/signin.html
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/signin.html
Method	POST
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://zero.webappsecurity.com/signin.html
Method	POST
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://zero.webappsecurity.com/signin.html
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	

Other Info	
URL	http://zero.webappsecurity.com/signin.html
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/signin.html
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://zero.webappsecurity.com/signin.html
Method	POST
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://zero.webappsecurity.com/signin.html
Method	POST
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://zero.webappsecurity.com/signin.html
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	96
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104