



ZAP by  
Checkmarx

# ZAP by Checkmarx Scanning Report

Site: <https://alfasearch.it>

Generated on Wed, 19 Mar 2025 10:31:28

ZAP Version: 2.16.0

ZAP by [Checkmarx](#)

## Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	5
Informational	8

## Alerts

Name	Risk Level	Number of Instances
<a href="#">Absence of Anti-CSRF Tokens</a>	Medium	1
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	9
<a href="#">Hidden File Found</a>	Medium	4
<a href="#">Vulnerable JS Library</a>	Medium	1
<a href="#">Cookie No HttpOnly Flag</a>	Low	3
<a href="#">Cookie Without Secure Flag</a>	Low	3
<a href="#">Private IP Disclosure</a>	Low	1
<a href="#">Strict-Transport-Security Header Not Set</a>	Low	16
<a href="#">X-Content-Type-Options Header Missing</a>	Low	7
<a href="#">Authentication Request Identified</a>	Informational	2
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	2
<a href="#">Modern Web Application</a>	Informational	4
<a href="#">Re-examine Cache-control Directives</a>	Informational	4
<a href="#">Session Management Response Identified</a>	Informational	6
<a href="#">Tech Detected - Django</a>	Informational	1
<a href="#">Tech Detected - Nginx</a>	Informational	1
<a href="#">User Agent Fuzzer</a>	Informational	60

## Alert Detail

---

Medium	Absence of Anti-CSRF Tokens
Description	<p>No Anti-CSRF tokens were found in a HTML submission form.</p> <p>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.</p> <p>CSRF attacks are effective in a number of situations, including:</p> <ul style="list-style-type: none"> <li>* The victim has an active session on the target site.</li> <li>* The victim is authenticated via HTTP auth on the target site.</li> <li>* The victim is on the same local network as the target site.</li> </ul> <p>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.</p>
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/spid">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/spid</a>
Method	GET
Attack	
Evidence	<pre>&lt;form action="https://spid.hmsbox.it/login" id="redirectForm" method="post" target="_self"&gt;</pre>
Other Info	<p>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: "loginUrl" "logoutUrl" ].</p>
Instances	1
Solution	<p>Phase: Architecture and Design</p> <p>Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.</p> <p>For example, use anti-CSRF packages such as the OWASP CSRFGuard.</p> <p>Phase: Implementation</p> <p>Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.</p> <p>Phase: Architecture and Design</p> <p>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).</p> <p>Note that this can be bypassed using XSS.</p> <p>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.</p> <p>Note that this can be bypassed using XSS.</p> <p>Use the ESAPI Session Management control.</p> <p>This control includes a component for CSRF.</p>

	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	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html</a> <a href="https://cwe.mitre.org/data/definitions/352.html">https://cwe.mitre.org/data/definitions/352.html</a>
CWE Id	<a href="#">352</a>
WASC Id	9
Plugin Id	<a href="#">10202</a>

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	<a href="https://alfasearch.it/">https://alfasearch.it/</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/api/">https://alfasearch.it/api/</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/api/accounts/me/">https://alfasearch.it/api/accounts/me/</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
Method	GET

Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/spid">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/spid</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/sitemap.xml">https://alfasearch.it/sitemap.xml</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/">https://alfasearch.it/</a>
Method	POST
Attack	
Evidence	
Other Info	
Instances	9
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy">https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy</a> <a href="https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html</a> <a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://w3c.github.io/webappsec-csp/">https://w3c.github.io/webappsec-csp/</a> <a href="https://web.dev/articles/csp">https://web.dev/articles/csp</a> <a href="https://caniuse.com/#feat=contentsecuritypolicy">https://caniuse.com/#feat=contentsecuritypolicy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10038</a>

<b>Medium</b>	<b>Hidden File Found</b>
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	<a href="https://alfasearch.it/.darcs">https://alfasearch.it/.darcs</a>
Method	GET
Attack	
Evidence	HTTP/1.1 204 No Content
Other Info	
URL	<a href="https://alfasearch.it/.bzs">https://alfasearch.it/.bzs</a>
Method	GET
Attack	
Evidence	HTTP/1.1 204 No Content
Other Info	
URL	<a href="https://alfasearch.it/.hg">https://alfasearch.it/.hg</a>
Method	GET
Attack	
Evidence	HTTP/1.1 204 No Content
Other Info	
URL	<a href="https://alfasearch.it/BitKeeper">https://alfasearch.it/BitKeeper</a>
Method	GET
Attack	
Evidence	HTTP/1.1 204 No Content
Other Info	
Instances	4
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	<a href="https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html">https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html</a>
CWE Id	<a href="#">538</a>
WASC Id	13
Plugin Id	<a href="#">40035</a>

<b>Medium</b>	<b>Vulnerable JS Library</b>
Description	The identified library appears to be vulnerable.
URL	<a href="https://alfasearch.it/js/chunk-vendors.1c97dee1.js">https://alfasearch.it/js/chunk-vendors.1c97dee1.js</a>
Method	GET
Attack	
Evidence	<pre>="3.4.1",w=function(e,t){return new w.fn.init(e,t)},H=/^\[\s\uFEFF\xA0]+\[\s\uFEFF\xA0]+\$/g;function k(e){var t=!!e&amp;&amp;"length"in e&amp;&amp;e.length,n=L(e);return!g(e)&amp;&amp;!M(e)&amp;&amp;("array"===n  0===t  "number"===typeof t&amp;&amp;t&gt;0&amp;&amp;t-1 in e)}w.fn=w.prototype={jquery:</pre>
Other Info	The identified library jquery, version 3.4.1 is vulnerable. CVE-2020-11023 CVE-2020-11022 <a href="https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/">https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/</a>
Instances	1
Solution	Upgrade to the latest version of the affected library.

Reference	<a href="https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/">https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/</a>
CWE Id	<a href="#">1395</a>
WASC Id	
Plugin Id	<a href="#">10003</a>

<b>Low</b>	<b>Cookie No HttpOnly Flag</b>
------------	--------------------------------

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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
-----	---

Method	GET
--------	-----

Attack	
--------	--

Evidence	Set-Cookie: csrftoken
----------	-----------------------

Other Info	
------------	--

URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
-----	---

Method	GET
--------	-----

Attack	
--------	--

Evidence	Set-Cookie: csrftoken
----------	-----------------------

Other Info	
------------	--

URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
-----	---

Method	GET
--------	-----

Attack	
--------	--

Evidence	Set-Cookie: csrftoken
----------	-----------------------

Other Info	
------------	--

Instances	3
-----------	---

Solution	Ensure that the HttpOnly flag is set for all cookies.
----------	---

Reference	<a href="https://owasp.org/www-community/HttpOnly">https://owasp.org/www-community/HttpOnly</a>
-----------	---

CWE Id	<a href="#">1004</a>
--------	----------------------

WASC Id	13
---------	----

Plugin Id	<a href="#">10010</a>
-----------	-----------------------

<b>Low</b>	<b>Cookie Without Secure Flag</b>
------------	-----------------------------------

Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
-------------	---

URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
-----	---

Method	GET
--------	-----

Attack	
--------	--

Evidence	Set-Cookie: csrftoken
----------	-----------------------

Other Info	
------------	--

URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
-----	---

Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
Instances	3
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	<a href="https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html">https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html</a>
CWE Id	<a href="#">614</a>
WASC Id	13
Plugin Id	<a href="#">10011</a>

<b>Low</b>	<b>Private IP Disclosure</b>
------------	------------------------------

Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	<a href="https://alfasearch.it/js/chunk-vendors.1c97dee1.js">https://alfasearch.it/js/chunk-vendors.1c97dee1.js</a>
Method	GET
Attack	
Evidence	10.1.9.34
Other Info	10.1.9.34 10.8.1.1 10.8.1.1
Instances	1
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP /PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Reference	<a href="https://tools.ietf.org/html/rfc1918">https://tools.ietf.org/html/rfc1918</a>
CWE Id	<a href="#">497</a>
WASC Id	13
Plugin Id	<a href="#">2</a>

<b>Low</b>	<b>Strict-Transport-Security Header Not Set</b>
------------	---

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	<a href="https://alfasearch.it/">https://alfasearch.it/</a>
Method	GET
Attack	

Evidence	
Other Info	
URL	<a href="https://alfasearch.it/api/">https://alfasearch.it/api/</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/api/accounts/me/">https://alfasearch.it/api/accounts/me/</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/css/app.8515ee0a.css">https://alfasearch.it/css/app.8515ee0a.css</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/css/chunk-vendors.8dea7374.css">https://alfasearch.it/css/chunk-vendors.8dea7374.css</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/favicon.ico">https://alfasearch.it/favicon.ico</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/images/logo.svg">https://alfasearch.it/images/logo.svg</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	
Evidence	
Other	

Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/spid">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/spid</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/js/app.5b568389.js">https://alfasearch.it/js/app.5b568389.js</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/js/chunk-vendors.1c97dee1.js">https://alfasearch.it/js/chunk-vendors.1c97dee1.js</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/robots.txt">https://alfasearch.it/robots.txt</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/sitemap.xml">https://alfasearch.it/sitemap.xml</a>
Method	GET
Attack	
Evidence	
Other Info	

URL	<a href="https://alfasearch.it/">https://alfasearch.it/</a>
Method	POST
Attack	
Evidence	
Other Info	
Instances	16
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	<a href="https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html</a> <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a> <a href="https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security">https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security</a> <a href="https://caniuse.com/stricttransportsecurity">https://caniuse.com/stricttransportsecurity</a> <a href="https://datatracker.ietf.org/doc/html/rfc6797">https://datatracker.ietf.org/doc/html/rfc6797</a>
CWE Id	<a href="#">319</a>
WASC Id	15
Plugin Id	<a href="#">10035</a>

<b>Low</b>	<b>X-Content-Type-Options Header Missing</b>
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	<a href="https://alfasearch.it/css/app.8515ee0a.css">https://alfasearch.it/css/app.8515ee0a.css</a>
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	<a href="https://alfasearch.it/css/chunk-vendors.8dea7374.css">https://alfasearch.it/css/chunk-vendors.8dea7374.css</a>
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	<a href="https://alfasearch.it/favicon.ico">https://alfasearch.it/favicon.ico</a>
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	<a href="https://alfasearch.it/images/logo.svg">https://alfasearch.it/images/logo.svg</a>

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	<a href="https://alfasearch.it/js/app.5b568389.js">https://alfasearch.it/js/app.5b568389.js</a>
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	<a href="https://alfasearch.it/js/chunk-vendors.1c97dee1.js">https://alfasearch.it/js/chunk-vendors.1c97dee1.js</a>
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	<a href="https://alfasearch.it/robots.txt">https://alfasearch.it/robots.txt</a>
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.
Instances	7
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	<a href="https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)">https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)</a> <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10021</a>

<b>Informational</b>	<b>Authentication Request Identified</b>
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	<a href="https://alfasearch.it/">https://alfasearch.it/</a>

Method	POST
Attack	
Evidence	password1
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=password1 referer=https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2 /signup/ csrfToken=csrfmiddlewaretoken
URL	<a href="https://alfasearch.it/">https://alfasearch.it/</a>
Method	POST
Attack	
Evidence	password
Other Info	userParam=username userValue=foo-bar@example.com passwordParam=password referer=https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2 csrfToken=csrfmiddlewaretoken
Instances	2
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	<a href="https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/">https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10111</a>

<b>Informational</b>	<b>Information Disclosure - Suspicious Comments</b>
----------------------	---

Description	The response appears to contain suspicious comments which may help an attacker.
URL	<a href="https://alfasearch.it/js/app.5b568389.js">https://alfasearch.it/js/app.5b568389.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: <code>\bSELECT\b</code> and was detected in likely comment: <code>//alfasearch.atlassian.net/servicedesk/"))))))).call(this,t("1157")), "49f8":function(e,n){function t(e){var n=new Error("Canno", see evidence field for the suspicious comment /snippet.</code>
URL	<a href="https://alfasearch.it/js/chunk-vendors.1c97dee1.js">https://alfasearch.it/js/chunk-vendors.1c97dee1.js</a>
Method	GET
Attack	
Evidence	bug
Other Info	The following pattern was used: <code>\bBUG\b</code> and was detected in likely comment: <code>//,Nt={},It={}, Ft="*/".concat(""),Wt=r.createElement("a");function \$(t,e){return function(t,n){"string"!=typeof t&amp;&amp;(n=t,t="*");v", see evidence field for the suspicious comment/snippet.</code>
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	<a href="#">615</a>
WASC Id	13
Plugin Id	<a href="#">10027</a>

<b>Informational</b>	<b>Modern Web Application</b>
----------------------	-------------------------------

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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	
Evidence	<noscript><strong>We're sorry but client doesn't work properly without JavaScript enabled. Please enable it to continue.</strong></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
Method	GET
Attack	
	<pre> &lt;script type="text/javascript"&gt; window.paceOptions = { target: '#pace-container' }; /*! pace 1.0.2 https://github.com/HubSpot/pace/tree/v1.0.2 */ (function(){var a,b,c,d,e,f,g,h,i,j,k,l,m,n, o,p,q,r,s,t,u,v,w,x,y,z,A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X=[];slice,Y={}. hasOwnProperty,Z=function(a,b){function c(){this.constructor=a}for(var d in b)Y.call(b,d)&amp;&amp; (a[d]=b[d]);return c.prototype=b.prototype,a.prototype=new c,a.__super__=b.prototype,a,\$= [].indexOf  function(a){for(var b=0,c=this.length;c&gt;b;b++)if(b in this&amp;&amp;this[b]===a)return b; return-1};for(u={catchupTime:100,initialRate:.03,minTime:250,ghostTime:100, maxProgressPerFrame:20,easeFactor:1.25,startOnPageLoad:!0,restartOnPushState:!0, restartOnRequestAfter:500,target:"body",elements:{checkInterval:100,selectors:["body"]}, eventLag:{minSamples:10,sampleCount:3,lagThreshold:3},ajax:{trackMethods:["GET"], trackWebSockets:!0,ignoreURLs:[]},C=function(){var a;return null!=(a="undefined"!==typeof performance&amp;&amp;null!==performance&amp;&amp;"function"===typeof performance.now?performance. now():void 0)?a:+new Date},E=window.requestAnimationFrame  window. mozRequestAnimationFrame  window.webkitRequestAnimationFrame  window. msRequestAnimationFrame,t=window.cancelAnimationFrame  window. mozCancelAnimationFrame,null==E&amp;&amp;(E=function(a){return setTimeout(a,50)},t=function(a) {return clearTimeout(a)}),G=function(a){var b,c;return b=C(),(c=function(){var d;return d=C()- b,d&gt;=33?(b=C(),a(d,function(){return E(c)})):setTimeout(c,33-d))()},F=function(){var a,b,c; return c=arguments[0],b=arguments[1],a=3&lt;=arguments.length?X.call(arguments,2):[]," function"===typeof c[b]?c[b].apply(c,a):c[b],v=function(){var a,b,c,d,e,f,g;for(b=arguments[0], d=2&lt;=arguments.length?X.call(arguments,1):[],f=0,g=d.length;g&gt;f;f++)if(c=d[f])for(a in c)Y. call(c,a)&amp;&amp;(e=c[a],null!=b[a]&amp;&amp;"object"===typeof b[a]&amp;&amp;null!=e&amp;&amp;"object"===typeof e?v(b[a], e):b[a]=e);return b},q=function(a){var b,c,d,e,f;for(c=b=0,e=0,f=a.length;f&gt;e;e++)d=a[e], c+=Math.abs(d),b++;return c/b},x=function(a,b){var c,d,e;if(null==a&amp;&amp;(a="options"), null==b&amp;&amp;(b=!0),e=document.querySelector("[data-pace-"+a+""])}{if(c=e.getAttribute("data- pace-"+a),!b)return c;try{return JSON.parse(c)}catch(f){return d=f,"undefined"!==typeof console&amp;&amp;null!==console?console.error("Error parsing inline pace options",d):void 0}}, g=function(){function a(){return a.prototype.on=function(a,b,c,d){var e;return null==d&amp;&amp;(d=! 1),null==this.bindings&amp;&amp;(this.bindings={}),null==(e=this.bindings)[a]&amp;&amp;(e[a]=[]),this.bindings [a].push({handler:b,ctx:c,once:d})},a.prototype.once=function(a,b,c){return this.on(a,b,c,!0)}, a.prototype.off=function(a,b){var c,d,e;if(null!=(d=this.bindings)?d[a]:void 0)}{if (null==b)return delete this.bindings[a];for(c=0,e=[];c&lt;this.bindings[a].length;)e.push(this. bindings[a][c].handler===b?this.bindings[a].splice(c,1):c++);return e},a.prototype. trigger=function(){var a,b,c,d,e,f,g,h,i;if(c=arguments[0],a=2&lt;=arguments.length?X.call (arguments,1):[],null!=(g=this.bindings)?g[c]:void 0)}{for(e=0,i=[];e&lt;this.bindings[c].length;) h=this.bindings[c][e],d=h.handler,b=h.ctx,f=h.once,d.apply(null!=b?b:this,a),i.push(f?this. bindings[c].splice(e,1):e++);return i},a()},{j=window.Pace  {}},window.Pace=j,v(j.g.prototype), D=j.options=v({},u,window.paceOptions,x()),U=["ajax","document","eventLag","elements"], Q=0,S=U.length;S&gt;Q;Q++)K=U[Q],D[K]=!0&amp;&amp;(D[K]=u[K]);i=function(a){function b(){return V=b.__super__.constructor.apply(this,arguments)}return Z(b,a),b}(Error),b=function() {function a(){this.progress=0}return a.prototype.getElement=function(){var a;if(null==this.el) {if(a=document.querySelector(D.target),!a)throw new i;this.el=document.createElement ("div"),this.el.className="pace pace-active",document.body.className=document.body. className.replace(/pace-done/g,""),document.body.className+=" pace-running",this.el. innerHTML='&lt;div class="pace-progress"&gt;\n &lt;div class="pace-progress-inner"&gt;&lt;/div&gt;\n&lt; /div&gt;\n&lt;div class="pace-activity"&gt;&lt;/div&gt;',null!=a.firstChild?a.insertBefore(this.el,a.firstChild): a.appendChild(this.el)}return this.el},a.prototype.finish=function(){var a;return a=this. getElement(),a.className=a.className.replace("pace-active",""),a.className+=" pace- inactive",document.body.className=document.body.className.replace("pace-running",""), document.body.className+=" pace-done"},a.prototype.update=function(a){return this. progress=a,this.render()},a.prototype.destroy=function(){try{this.getElement().parentNode. </pre>

Evidence

```
removeChild(this.getElement())catch(a){i=a}return this.el=void 0},a.prototype.  
render=function(){var a,b,c,d,e,f,g;if(null==document.querySelector(D.target))return!1;for  
(a=this.getElement(),d="translate3d("+this.progress+"%, 0, 0)",g=["webkitTransform", "  
msTransform", "transform"],e=0,f=g.length;f>e;e++)b=g[e],a.children[0].style[b]=d;return(!this.  
lastRenderedProgress||this.lastRenderedProgress[0]!=this.progress[0])&&(a.children[0].  
setAttribute("data-progress-text", ""+(0|this.progress)+"%"),this.progress>=100?c="99":  
(c=this.progress<10?"0":"",c+=0|this.progress),a.children[0].setAttribute("data-progress", ""  
+c)),this.lastRenderedProgress=this.progress},a.prototype.done=function(){return this.  
progress>=100},a},h=function(){function a(){this.bindings={}}return a.prototype.  
trigger=function(a,b){var c,d,e,f,g;if(null!=this.bindings[a]){for(f=this.bindings[a],g=[],d=0,e=f.  
length;e>d;d++)c=f[d],g.push(c.call(this,b));return g}},a.prototype.on=function(a,b){var c;  
return null==(c=this.bindings[a])&&(c[a]=[]),this.bindings[a].push(b),a}(),P=window.  
XMLHttpRequest,O=window.XDomainRequest,N=window.WebSocket,w=function(a,b){var c,  
d,e;e=[];for(d in b.prototype)try{e.push(null==a[d]&&"function"!=typeof b[d]?"function"  
==typeof Object.defineProperty?Object.defineProperty(a,d,{get:function(){return b.prototype  
[d]},configurable:!0,enumerable:!0}):a[d]=b.prototype[d]:void 0)}catch(f){c=f}return e},A=[],j.  
ignore=function(){var a,b,c;return b=arguments[0],a=2<=arguments.length?X.call  
(arguments,1):[],A.unshift("ignore"),c=b.apply(null,a),A.shift(),c},j.track=function(){var a,b,c;  
return b=arguments[0],a=2<=arguments.length?X.call(arguments,1):[],A.unshift("track"),c=b.  
apply(null,a),A.shift(),c},J=function(a){var b;if(null==a&&(a="GET"),"track"===A[0])return  
force;if(!A.length&&D.ajax){if("socket"===a&&D.ajax.trackWebSockets)return!0;if(b=a.  
toUpperCase(),$.call(D.ajax.trackMethods,b)>=0)return!0}return!1},k=function(a){function b()  
{var a,c=this;b.__super__.constructor.apply(this,arguments),a=function(a){var b;return b=a.  
open,a.open=function(d,e){return J(d)&&c.trigger("request",{type:d,url:e,request:a}),b.apply  
(a,arguments)},window.XMLHttpRequest=function(b){var c;return c=new P(b),a(c),c};try{w  
(window.XMLHttpRequest,P)}catch(d){if(null!=O){window.XDomainRequest=function(){var  
b;return b=new O,a(b),b};try{w(window.XDomainRequest,O)}catch(d){if(null!=N&&D.ajax.  
trackWebSockets){window.WebSocket=function(a,b){var d;return d=null!=b?new N(a,b):  
new N(a),J("socket")&&c.trigger("request",{type:"socket",url:a,protocols:b,request:d}),d};try{w  
(window.WebSocket,N)}catch(d){}}}}return Z(b,a),b}(h),R=null,y=function(){return null==R&&  
(R=new k),R},l=function(a){var b,c,d,e;for(e=D.ajax.ignoreURLs,c=0,d=e.length;d>c;c++)if  
(b=e[c],"string"==typeof b){if(-1!==a.indexOf(b))return!0}else if(b.test(a))return!0;return!1},y().  
on("request",function(b){var c,d,e,f,g;return f=b.type,e=b.request,g=b.url,l(g)?void 0:j.  
running||D.restartOnRequestAfter===!1&&"force"!==J(f)?void 0:(d=arguments,c=D.  
restartOnRequestAfter||0,"boolean"==typeof c&&(c=0),setTimeout(function(){var b,c,g,h,i,k;if  
(b="socket"===f?e.readyState<2:0<(h=e.readyState)&&4>h){for(j.restart(),i=j.sources,k=[],  
c=0,g=i.length;g>c;c++){if(K=i[c],K instanceof a){K.watch.apply(K,d);break}k.push(void 0)  
return k}},c)),a=function(){function a(){var a=this;this.elements=[],y().on("request",function()  
{return a.watch.apply(a,arguments)})}return a.prototype.watch=function(a){var b,c,d,e;return  
d=a.type,b=a.request,e=a.url,l(e)?void 0:(c="socket"===d?new n(b):new o(b),this.elements.  
push(c)),a}(),o=function(){function a(a){var b,c,d,e,f,g,h=this;if(this.progress=0,null!  
=window.ProgressEvent)for(c=null,a.addEventListener("progress",function(a){return h.  
progress=a.lengthComputable?100*a.loaded/a.total:h.progress+(100-h.progress)/2,!1}),g=  
["load","abort","timeout","error"],d=0,e=g.length;e>d;d++)b=g[d],a.addEventListener(b,  
function(){return h.progress=100,!1});else f=a.onreadystatechange,a.  
onreadystatechange=function(){var b;return 0===(b=a.readyState)||4===b?h.progress=100:  
3===a.readyState&&(h.progress=50),"function"==typeof f?f.apply(null,arguments):void 0}  
return a}(),n=function(){function a(a){var b,c,d,e,f=this;for(this.progress=0,e=["error","open"],  
c=0,d=e.length;d>c;c++)b=e[c],a.addEventListener(b,function(){return f.progress=100,!1})  
return a}(),d=function(){function a(a){var b,c,d,f;for(null==a&&(a={}),this.elements=[],null==a.  
selectors&&(a.selectors=[]),f=a.selectors,c=0,d=f.length;d>c;c++)b=f[c],this.elements.push  
(new e(b))}return a}(),e=function(){function a(a){this.selector=a,this.progress=0,this.check()  
return a.prototype.check=function(){var a=this;return document.querySelector(this.selector)?  
this.done():setTimeout(function(){return a.check()},D.elements.checkInterval)},a.prototype.  
done=function(){return this.progress=100},a}(),c=function(){function a(){var a,b,c=this;this.  
progress=null!=(b=this.states[document.readyState])?b:100,a=document.  
onreadystatechange,document.onreadystatechange=function(){return null!=c.states  
[document.readyState]&&(c.progress=c.states[document.readyState]),"function"==typeof a?  
a.apply(null,arguments):void 0}return a.prototype.states={loading:0,interactive:50,complete:  
100},a}(),f=function(){function a(a){var a,b,c,d,e,f=this;this.progress=0,a=0,e=[],d=0,c=C(),  
b=setInterval(function(){var g;return g=C()-c-50,c=C(),e.push(g),e.length>D.eventLag.  
sampleCount&&e.shift(),a=q(e),++d>=D.eventLag.minSamples&&a<D.eventLag.  
lagThreshold?(f.progress=100,clearInterval(b)):f.progress=100*(3/(a+3)),50)}return a}(),  
m=function(){function a(a){this.source=a,this.last=this.sinceLastUpdate=0,this.rate=D.  
initialRate,this.catchup=0,this.progress=this.lastProgress=0,null!=this.source&&(this.  
progress=F(this.source,"progress"))}return a.prototype.tick=function(a,b){var c;return  
null==b&&(b=F(this.source,"progress")),b>=100&&(this.done=!0),b===this.last?this.  
sinceLastUpdate+=a:(this.sinceLastUpdate&&(this.rate=(b-this.last)/this.sinceLastUpdate),
```

```
this.catchup=(b-this.progress)/D.catchupTime,this.sinceLastUpdate=0,this.last=b),b>this.progress&&(this.progress+=this.catchup*a),c=1-Math.pow(this.progress/100,D.easeFactor),this.progress+=c*this.rate*a,this.progress=Math.min(this.lastProgress+D.maxProgressPerFrame,this.progress),this.progress=Math.max(0,this.progress),this.progress=Math.min(100,this.progress),this.lastProgress=this.progress,this.progress},a)(),L=null,H=null,r=null,M=null,p=null,s=null,j.running=!1,z=function(){return D.restartOnPushState?j.restart():void 0},null!=window.history.pushState&&(T=window.history.pushState,window.history.pushState=function(){return z(),T.apply(window.history,arguments)}),null!=window.history.replaceState&&(W=window.history.replaceState,window.history.replaceState=function(){return z(),W.apply(window.history,arguments)}),l={ajax:a,elements:d,document:c,eventLag:f,(B=function(){var a,c,d,e,f,g,h,i;for(j.sources=L=[],g=["ajax","elements","document","eventLag"],c=0,e=g.length;e<c;c++)a=g[c],D[a]!=!1&&L.push(new l[a](D[a]));for(i=null!=(h=D.extraSources)?h:[],d=0,f=i.length;f>d;d++)K=i[d],L.push(new K(D));return j.bar=r=new b,H=[],M=new m)}(),j.stop=function(){return j.trigger("stop"),j.running=!1,r.destroy(),s=!0,null!=p&&("function"==typeof t&&t(p),p=null),B()},j.restart=function(){return j.trigger("restart"),j.stop(),j.start(),j.go=function(){var a;return j.running=!0,r.render(),a=C(),s=!1,p=G(function(b,c){var d,e,f,g,h,i,k,l,n,o,p,q,t,u,v,w;for(l=100-r.progress,e=p=0,f=!0,i=q=0,u=L.length;u>q;i=++q)for(K=L[i],o=null!=H[i]?H[i]:H[i]=[],h=null!=(w=K.elements)?w:[K],k=t=0,v=h.length;v>t;k=++t)g=h[k],n=null!=o[k]?o[k]:o[k]=new m(g),f&=n.done,n.done||(e=++p+=n.tick(b));return d=p/e,r.update(M.tick(b,d)),r.done()}|f|s?(r.update(100),j.trigger("done"),setTimeout(function(){return r.finish(),j.running=!1,j.trigger("hide"),Math.max(D.ghostTime,Math.max(D.minTime-(C()-a),0)):c)}),j.start=function(a){v(D,a),j.running=!0;try{r.render()}catch(b){i=b}return document.querySelector("pace")?(j.trigger("start"),j.go()):setTimeout(j.start,50),"function"==typeof define&&define.amd?define(["pace"],function(){return j}):"object"==typeof exports?module.exports=j:D.startOnPageLoad&&j.start()).call(this); Pace.once("done",function(){document.querySelector("#bodyBlockLoading").style.display="none";document.querySelector("#bodyBlock").style.display="block"; Pace.stop();}); </script>
```

Other Info No links have been found while there are scripts, which is an indication that this is a modern web application.

URL <https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/>

Method GET

Attack

```
<script type="text/javascript"> window.paceOptions = { target: '#pace-container' }; /*! pace 1.0.2 https://github.com/HubSpot/pace/tree/v1.0.2 */ (function(){var a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z,A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X=[].slice,Y={}.hasOwnProperty,Z=function(a,b){function c(){this.constructor=a}for(var d in b)Y.call(b,d)&&(a[d]=b[d]);return c.prototype=b.prototype,a.prototype=new c,a.__super__=b.prototype,a}$.indexof=function(a){for(var b=0,c=this.length;c>b;b++)if(b in this&&this[b]===a)return b;return-1};for(u={catchupTime:100,initialRate:.03,minTime:250,ghostTime:100,maxProgressPerFrame:20,easeFactor:1.25,startOnPageLoad:!0,restartOnPushState:!0,restartOnRequestAfter:500,target:"body",elements:{checkInterval:100,selectors:["body"]},eventLag:{minSamples:10,sampleCount:3,lagThreshold:3},ajax:{trackMethods:["GET"],trackWebSockets:!0,ignoreURLs:[]},C=function(){var a;return null!=(a="undefined"!=typeof performance&&null!=performance&&"function"==typeof performance.now?performance.now():void 0)?a:+new Date),E=window.requestAnimationFrame||window.mozRequestAnimationFrame||window.webkitRequestAnimationFrame||window.msRequestAnimationFrame,t=window.cancelAnimationFrame||window.mozCancelAnimationFrame,null==E&&(E=function(a){return setTimeout(a,50)},t=function(a){return clearTimeout(a)},G=function(a){var b,c;return b=C(),(c=function(){var d;return d=C()-b,d>=33?(b=C(),a(d,function(){return E(c)})):setTimeout(c,33-d)}()),F=function(){var a,b,c;return c=arguments[0],b=arguments[1],a=3<=arguments.length?X.call(arguments,2):[],"function"==typeof c[b]?c[b].apply(c,a):c[b],v=function(){var a,b,c,d,e,f,g;for(b=arguments[0],d=2<=arguments.length?X.call(arguments,1):[],f=0,g=d.length;g>f;f++)if(c=d[f])for(a in c)Y.call(c,a)&&(e=c[a],null!=b[a]&&"object"==typeof b[a]&&null!=e&&"object"==typeof e?v(b[a],e):b[a]=e);return b},q=function(a){var b,c,d,e,f;for(c=b=0,e=0,f=a.length;f>e;e++)d=a[e],c+=Math.abs(d),b++;return c/b},x=function(a,b){var c,d,e;if(null==a&&(a="options"),null==b&&(b=!0),e=document.querySelector("[data-pace-"+a+""])}(if(c=e.getAttribute("data-pace-"+a),!b)return c;try{return JSON.parse(c)}catch(f){return d=f,"undefined"!=typeof console&&null!=console?console.error("Error parsing inline pace options",d):void 0}},g=function(){function a(){return a.prototype.on=function(a,b,c,d){var e;return null==d&&(d=!1),null==this.bindings&&(this.bindings={}),null==(e=this.bindings)[a]&&(e[a]=[]),this.bindings[a].push({handler:b,ctx:c,once:d}),a.prototype.once=function(a,b,c){return this.on(a,b,c,!0)},a.prototype.off=function(a,b){var c,d,e;if(null!=(null!=(d=this.bindings)?d[a]:void 0)}(if(null==b)return delete this.bindings[a];for(c=0,e=[];c<this.bindings[a].length;)e.push(this.
```

Evidence

```
bindings[a][c].handler===b?this.bindings[a].splice(c,1):c++;return e}},a.prototype.  
trigger=function(){var a,b,c,d,e,f,g,h,i;if(c=arguments[0],a=2<=arguments.length?X.call  
(arguments,1):[],null!=(g=this.bindings)?g[c]:void 0){for(e=0,i=[];e<this.bindings[c].length;)h=this.bindings[c][e],d=h.handler,b=h.ctx,f=h.once,d.apply(null!=b?this,a),i.push(f?this.bindings[c].splice(e,1):e++);return i}},a().j=window.Pace||{,window.Pace=j,v(j,g.prototype),D=j.options=v({},u,window.paceOptions,x()),U=["ajax","document","eventLag","elements"],Q=0,S=U.length;S>Q;Q++)K=U[Q],D[K]===!0&&(D[K]=u[K]);i=function(a){function b(){return V=b.__super__.constructor.apply(this,arguments)}return Z(b,a),b}(Error),b=function(){function a(){this.progress=0}return a.prototype.getElement=function(){var a;if(null==this.el){if(a=document.querySelector(D.target),!a)throw new i;this.el=document.createElement("div"),this.el.className="pace pace-active",document.body.className=document.body.className.replace(/pace-done/g,""),document.body.className+=" pace-running",this.el.innerHTML='<div class="pace-progress">\n <div class="pace-progress-inner"></div>\n</div>\n<div class="pace-activity"></div>',null!=a.firstChild?a.insertBefore(this.el,a.firstChild):a.appendChild(this.el)}return this.el},a.prototype.finish=function(){var a;return a=this.getElement(),a.className=a.className.replace("pace-active",""),a.className+=" pace-inactive",document.body.className=document.body.className.replace("pace-running",""),document.body.className+=" pace-done"},a.prototype.update=function(a){return this.progress=a,this.render()},a.prototype.destroy=function(){try{this.getElement().parentNode.removeChild(this.getElement())}catch(a){i=a}return this.el=void 0},a.prototype.render=function(){var a,b,c,d,e,f,g;if(null==document.querySelector(D.target))return!1;for(a=this.getElement(),d="translate3d("+this.progress+"%, 0, 0)",g=["webkitTransform","msTransform","transform"],e=0,f=g.length;f>e;e++)b=g[e],a.children[0].style[b]=d;return(!this.lastRenderedProgress||this.lastRenderedProgress[0]!=this.progress[0]&&(a.children[0].setAttribute("data-progress-text",""+(0|this.progress)+"%"),this.progress>=100?c="99":(c=this.progress<10?"0":"",c+=0|this.progress),a.children[0].setAttribute("data-progress",""+c)),this.lastRenderedProgress=this.progress},a.prototype.done=function(){return this.progress>=100},a().h=function(a){function a(){this.bindings={}}return a.prototype.trigger=function(a,b){var c,d,e,f,g;if(null!=this.bindings[a]){for(f=this.bindings[a],g=[],d=0,e=f.length;e>d;d++)c=f[d],g.push(c.call(this,b));return g}},a.prototype.on=function(a,b){var c;return null==(c=this.bindings[a]&&(c[a]=[]),this.bindings[a].push(b)),a().P=window.XMLHttpRequest,O=window.XDomainRequest,N=window.WebSocket,w=function(a,b){var c,d,e;e=[];for(d in b.prototype)try{e.push(null==a[d]&&"function"!=typeof b[d]?"function"==typeof Object.defineProperty?Object.defineProperty(a,d,{get:function(){return b.prototype[d]},configurable:!0,enumerable:!0}):a[d]=b.prototype[d]:void 0)}catch(f){c=f}return e},A=[],j.ignore=function(){var a,b,c;return b=arguments[0],a=2<=arguments.length?X.call(arguments,1):[],A.unshift("ignore"),c=b.apply(null,a),A.shift(),c},j.track=function(){var a,b,c;return b=arguments[0],a=2<=arguments.length?X.call(arguments,1):[],A.unshift("track"),c=b.apply(null,a),A.shift(),c},J=function(a){var b;if(null==a&&(a="GET"),"track"===A[0])return"force";if(!A.length&&D.ajax){if("socket"===a&&D.ajax.trackWebSockets)return!0;if(b=a.toUpperCase(),$.call(D.ajax.trackMethods,b)>=0)return!0}return!1},k=function(a){function b(){var a,c=this;b.__super__.constructor.apply(this,arguments),a=function(a){var b;return b=a.open,a.open=function(d,e){return J(d)&&c.trigger("request",{type:d,url:e,request:a}),b.apply(a,arguments)}},window.XMLHttpRequest&&c.trigger=function(b){var c;return c=new P(b,a(c),c);try{w(window.XMLHttpRequest,P)}catch(d){}if(null!=O){window.XDomainRequest&&c.trigger(function(){var b;return b=new O,a(b),b};try{w(window.XDomainRequest,O)}catch(d){}if(null!=N&&D.ajax.trackWebSockets){window.WebSocket=function(a,b){var d;return d=null!=b?new N(a,b):new N(a),J("socket")&&c.trigger("request",{type:"socket",url:a,protocols:b,request:d}),d};try{w(window.WebSocket,N)}catch(d){}}return Z(b,a),b}(h),R=null,y=function(){return null==R&&(R=new k),R},l=function(a){var b,c,d,e;for(e=D.ajax.ignoreURLs,c=0,d=e.length;d>c;c++)if(b=e[c],"string"==typeof b){if(-1==a.indexOf(b))return!0}else if(b.test(a))return!0;return!1},y().on("request",function(b){var c,d,e,f,g;return f=b.type,e=b.request,g=b.url,l(g)?void 0:j.running||D.restartOnRequestAfter===!1&&"force"!=J(f)?void 0:(d=arguments,c=D.restartOnRequestAfter||0,"boolean"==typeof c&&(c=0),setTimeout(function(){var b,c,g,h,i,k;if(b="socket"===f?e.readyState<2:0<(h=e.readyState)&&4>h){for(j.restart(),i=j.sources,k=[],c=0,g=i.length;g>c;c++){if(K=i[c],K instanceof a){K.watch.apply(K,d);break}k.push(void 0)}return k}},c)),a=function(){function a(){var a=this;this.elements=[],y().on("request",function(){return a.watch.apply(a,arguments)}))return a.prototype.watch=function(a){var b,c,d,e;return d=a.type,b=a.request,e=a.url,l(e)?void 0:(c="socket"===d?new n(b):new o(b),this.elements.push(c)),a().o=function(a){function a(a){var b,c,d,e,f,g,h=this;if(this.progress=0,null!=window.ProgressEvent)for(c=null,a.addEventListeners("progress",function(a){return h.progress=a.lengthComputable?100*a.loaded/a.total:h.progress+(100-h.progress)/2},!1),g=["load","abort","timeout","error"],d=0,e=g.length;e>d;d++)b=g[d],a.addEventListener(b,function(){return h.progress=100},!1);else f=a.onreadystatechange,a.onreadystatechange=function(){var b;return 0===(b=a.readyState)||4===b?h.progress=100:3===a.readyState&&(h.progress=50),"function"==typeof f?f.apply(null,arguments):void 0}}return a},n=function(){function a(a){var b,c,d,e,f=this;for(this.progress=0,e=["error","open"],c=0,d=e.length;d>c;c++)b=e[c],a.addEventListener(b,function(){return f.progress=100},!1)}
```

```

return a}(),d=function(){function a(a){var b,c,d,f;for(null==a&&(a={}),this.elements=[],null==a.selectors&&(a.selectors=[]),f=a.selectors,c=0,d=f.length;d>c;c++)b=f[c],this.elements.push(new e(b));return a}(),e=function(){function a(a){this.selector=a,this.progress=0,this.check()}return a.prototype.check=function(){var a=this;return document.querySelector(this.selector)?this.done():setTimeout(function(){return a.check()},D.elements.checkInterval)},a.prototype.done=function(){return this.progress=100},a}(),c=function(){function a(){var a,b,c=this;this.progress=null!=(b=this.states[document.readyState])?b:100,a=document.onreadystatechange=document.onreadystatechange=function(){return null!=c.states[document.readyState]&&(c.progress=c.states[document.readyState]),"function"==typeof a?a.apply(null,arguments):void 0}return a.prototype.states={loading:0,interactive:50,complete:100},a}(),f=function(){function a(){var a,b,c,d,e,f=this;this.progress=0,a=0,e=[],d=0,c=C(),b=setInterval(function(){var g;return g=C()-c-50,c=C(),e.push(g),e.length>D.eventLag.sampleCount&&e.shift(),a=q(e),++d>=D.eventLag.minSamples&&a<D.eventLag.lagThreshold?(f.progress=100,clearInterval(b)):f.progress=100*(3/(a+3)),50)}return a}(),m=function(){function a(a){this.source=a,this.last=this.sinceLastUpdate=0,this.rate=D.initialRate,this.catchup=0,this.progress=this.lastProgress=0,null!=this.source&&(this.progress=F(this.source,"progress"))}return a.prototype.tick=function(a,b){var c;return null==b&&(b=F(this.source,"progress")),b>=100&&(this.done=!0),b===this.last?this.sinceLastUpdate+=a:(this.sinceLastUpdate&&(this.rate=(b-this.last)/this.sinceLastUpdate),this.catchup=(b-this.progress)/D.catchupTime,this.sinceLastUpdate=0,this.last=b),b>this.progress&&(this.progress+=this.catchup*a),c=1-Math.pow(this.progress/100,D.easeFactor),this.progress+=c*this.rate*a,this.progress=Math.min(this.lastProgress+D.maxProgressPerFrame,this.progress),this.progress=Math.max(0,this.progress),this.progress=Math.min(100,this.progress),this.lastProgress=this.progress,this.progress},a}(),L=null,H=null,r=null,M=null,p=null,s=null,j.running=!1,z=function(){return D.restartOnPushState?j.restart():void 0},null!=window.history.pushState&&(T=window.history.pushState,window.history.pushState=function(){return z(),T.apply(window.history,arguments)}),null!=window.history.replaceState&&(W=window.history.replaceState,window.history.replaceState=function(){return z(),W.apply(window.history,arguments)}),l={ajax:a,elements:d,document:c,eventLag:f},{B=function(){var a,c,d,e,f,g,h,i;for(j.sources=L=[],g=["ajax","elements","document","eventLag"],c=0,e=g.length;e>c;c++)a=g[c],D[a]!==!1&&L.push(new l[a](D[a]));for(i=null!=(h=D.extraSources)?h:[],d=0,f=i.length;f>d;d++)K=i[d],L.push(new K(D));return j.bar=r=new b,H=[],M=new m}(),j.stop=function(){return j.trigger("stop"),j.running=!1,r.destroy(),s=!0,null!=p&&("function"==typeof t&&t(p),p=null),B()}},j.restart=function(){return j.trigger("restart"),j.stop(),j.start(),j.go=function(){var a;return j.running=!0,r.render(),a=C(),s=!1,p=G(function(b,c){var d,e,f,g,h,i,k,l,n,o,p,q,t,u,v,w;for(l=100-r.progress,e=p=0,f=!0,i=q=0,u=L.length;u>q;i=++q)for(K=L[i],o=null!=H[i]?H[i]:H[i]=[],h=null!=(w=K.elements)?w:[K],k=t=0,v=h.length;v>t;k=++t)g=h[k],n=null!=o[k]?o[k]:o[k]=new m(g),f&=n.done,n.done||(e++,p+=n.tick(b));return d=p/e,r.update(M.tick(b,d)),r.done()||f||s?(r.update(100),j.trigger("done"),setTimeout(function(){return r.finish(),j.running=!1,j.trigger("hide"),Math.max(D.ghostTime,Math.max(D.minTime-(C()-a),0)))):c()}),j.start=function(a){v(D,a),j.running=!0;try{r.render()}catch(b){i=b}return document.querySelector(".pace")?(j.trigger("start"),j.go()):setTimeout(j.start,50)},"function"==typeof define&&define.amd?define(["pace"],function(){return j}):"object"==typeof exports?module.exports=j:D.startOnPageLoad&&j.start()}).call(this); Pace.once("done",function(){document.querySelector("#bodyBlockLoading").style.display="none";document.querySelector("#bodyBlock").style.display="block";Pace.stop();}); </script>

```

Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/spid">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/spid</a>
Method	GET
Attack	
Evidence	<script type="text/javascript"> document.getElementById("redirectForm").submit(); </script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	4
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	<a href="#">10109</a>

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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/spid">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/spid</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/robots.txt">https://alfasearch.it/robots.txt</a>
Method	GET
Attack	
Evidence	
Other Info	
Instances	4
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	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching">https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching</a> <a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control</a> <a href="https://grayduck.mn/2021/09/13/cache-control-recommendations/">https://grayduck.mn/2021/09/13/cache-control-recommendations/</a>
CWE Id	<a href="#">525</a>
WASC Id	13
Plugin Id	<a href="#">10015</a>

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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	
Evidence	4oEOx6KQfkmlWOUZLFi5bTYmeMoUWLKS
Other Info	cookie:csrftoken cookie:sessionid
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	
Evidence	GUEK9io5vyFV7I56JgQ25U0qceuP4dj1
Other Info	cookie:csrftoken cookie:sessionid
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	
Evidence	e5J1M1y3cqWqzY73Mg39qq3uVRIQViZ3
Other Info	cookie:csrftoken cookie:sessionid
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	
Evidence	mxGrDg1ohNB3KNuy0xj6mEpFpkFzhV4T
Other Info	cookie:csrftoken cookie:sessionid
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
Method	GET
Attack	
Evidence	4oEOx6KQfkmlWOUZLFi5bTYmeMoUWLKS
Other Info	cookie:csrftoken
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
Method	GET
Attack	
Evidence	4oEOx6KQfkmlWOUZLFi5bTYmeMoUWLKS
Other Info	cookie:csrftoken
Instances	6
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	<a href="https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id">https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10112</a>

Informational

Tech Detected - Django

Description	The following "Web frameworks" technology was identified: Django. Described as: Django is a Python-based free and open-source web application framework.
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	
Evidence	<input name="csrfmiddlewaretoken" type="hidden" value="as6K8yX7iMYygITTRCZuknrX9b9dmWWnmPC1BEOlpppRQldhHZ8qwRGsolECtHQ6"/>
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:djangoproject:django:*:*:*:*:*
Instances	1
Solution	
Reference	<a href="https://djangoproject.com">https://djangoproject.com</a>
CWE Id	
WASC Id	13
Plugin Id	<a href="#">10004</a>

<b>Informational</b>	<b>Tech Detected - Nginx</b>
----------------------	------------------------------

Description	The following "Web servers, Reverse proxies" technology was identified: Nginx. Described as: Nginx is a web server that can also be used as a reverse proxy, load balancer, mail proxy and HTTP cache.
URL	<a href="https://alfasearch.it/robots.txt">https://alfasearch.it/robots.txt</a>
Method	GET
Attack	
Evidence	nginx
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:f5:nginx:*:*:*:*:*
Instances	1
Solution	
Reference	<a href="https://nginx.org/en">https://nginx.org/en</a>
CWE Id	
WASC Id	13
Plugin Id	<a href="#">10004</a>

<b>Informational</b>	<b>User Agent Fuzzer</b>
----------------------	--------------------------

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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	

URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>

Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	

URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	

URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/password_reset/</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
Method	GET

Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
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	<a href="https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/">https://alfasearch.it/jobRequestBulletin/7b6e4074-9f16-4799-9b65-310a28a38ea2/signup/</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	60
Solution	
Reference	<a href="https://owasp.org/wstg">https://owasp.org/wstg</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10104</a>