ZAP Scanning Report

Sites: https://www.googletagmanager.com https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://calendar.ndbbank.com

Generated on Tue, 11 Jun 2024 12:03:06

ZAP Version: 2.14.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	5
Informational	8

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	3
Cross-Domain Misconfiguration	Medium	4
Vulnerable JS Library	Medium	3
Cookie No HttpOnly Flag	Low	2
Cookie Without Secure Flag	Low	4
Cross-Domain JavaScript Source File Inclusion	Low	6
Strict-Transport-Security Header Not Set	Low	20
X-Content-Type-Options Header Missing	Low	19
Information Disclosure - Sensitive Information in URL	Informational	1
Information Disclosure - Suspicious Comments	Informational	20
Modern Web Application	Informational	2
Re-examine Cache-control Directives	Informational	3
Retrieved from Cache	Informational	5
Session Management Response Identified	Informational	37
User Agent Fuzzer	Informational	12
User Controllable HTML Element Attribute (Potential XSS)	Informational	2

Alert Detail

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 cer types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks used for everything from data theft to site defacement or distribution of malware. CSP provides of standard HTTP headers that allow website owners to declare approved sources of content th 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
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/?_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Cont Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Poli 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	https://cdn.jsdelivr.net/jquery.validation/1.15.0/additional-methods.min.js
Method	GET
Attack	
Evidence	access-control-allow-origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could

	be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery-validate/1.19.3/jquery.validate.min.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdnjs.cloudflare.com/ajax/libs/MaterialDesign-Webfont/3.0.39/css/materialdesignicons.min.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PL84FQZT
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	4
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Medium	**Vulnerable JS Library**
Description	The identified library jquery-validation, version 1.19.5 is vulnerable.
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js
Method	GET
Attack	

Evidence	/*! * jQuery Validation Plugin v1.19.5
Other Info	
URL	https://cdn.jsdelivr.net/jquery.validation/1.15.0/additional-methods.min.js
Method	GET
Attack	
Evidence	/*! jQuery Validation Plugin - v1.15.0
Other Info	CVE-2022-31147 CVE-2021-21252 CVE-2021-43306
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery-validate/1.19.3/jquery.validate.min.js
Method	GET
Attack	
Evidence	/1.19.3/jquery.validate.min.js
Other Info	CVE-2022-31147 CVE-2021-43306
Instances	3
Solution	Please upgrade to the latest version of jquery-validation.
Reference	https://github.com/jquery-validation/jquery-validation/blob/master/changelog.md#1200--2023-10-10
CWE Id	829
WASC Id	
Plugin Id	10003

Low	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed JavaScript. If a malicious script can be run on this page then the cookie will be accessible and c transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://calendar.ndbbank.com/?_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
Instances	2
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	Cookie Without Secure Flag
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed vi unencrypted connections.
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	Set-Cookie: ndb_session
Other Info	
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://calendar.ndbbank.com/?_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	Set-Cookie: ndb_session
Other Info	
URL	https://calendar.ndbbank.com/?_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
Instances	4
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always b passed using an encrypted channel. Ensure that the secure flag is set for cookies containing su sensitive information.
Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Tes /06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html
CWE Id	614
WASC Id	13
Plugin Id	10011

Low	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/jquery.validation/1.15.0/additional-methods.min.js"></script>
Other	

Info	
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-validate/1.19.3/jquery.validate.min.js"> /script>
Other Info	
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=G-XJ2EHFVWPM"></script>
Other Info	
URL	https://calendar.ndbbank.com/? _token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/jquery.validation/1.15.0/additional-methods.min.js"></script>
Other Info	
URL	https://calendar.ndbbank.com/? _token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-validate/1.19.3/jquery.validate.min.js"> /script>
Other Info	
URL	https://calendar.ndbbank.com/? _token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=G-XJ2EHFVWPM"></script>
Other Info	
Instances	6
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Low	**Strict-Transport-Security Header Not Set**

Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web serv declares that complying user agents (such as a web browser) are to interact with it using only se HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protoc and is specified in RFC 6797.
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/?_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/admin/images/background-desktop-img.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/favicon.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/public/admin/css/vertical-layout-light/style.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/public/admin/fonts/Roboto/Roboto-Light.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/public/admin/fonts/Roboto/Roboto-Regular.woff2
Method	GET
Attack	
Evidence	

Other Info	
URL	https://calendar.ndbbank.com/public/admin/images/ndb-logo.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/public/admin/images/NDB-Logo_White.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/public/admin/js/hoverable-collapse.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/public/admin/js/off-canvas.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/public/admin/js/settings.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/public/admin/js/template.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/public/admin/js/todolist.js
Method	GET
Attack	
Evidence	
Other Info	

URL	https://calendar.ndbbank.com/public/admin/vendors/css/vendor.bundle.base.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/public/admin/vendors/js/vendor.bundle.base.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/public/admin/vendors/sweetalert/sweetalert.min.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	20
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Stri Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15

Plugin Id	10035

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows olde versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, poter causing the response body to be interpreted and displayed as a content type other than the dec content type. Current (early 2014) and legacy versions of Firefox will use the declared content ty one is set), rather than performing MIME-sniffing.
URL	https://calendar.ndbbank.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 affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/?_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/admin/images/background-desktop-img.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 affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/css/vertical-layout-light/style.css
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/fonts/Roboto/Roboto-Light.woff2
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/fonts/Roboto/Roboto-Regular.woff2
Method	GET
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/images/ndb-logo.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/images/NDB-Logo_White.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/js/hoverable-collapse.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 affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/js/off-canvas.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 affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/js/settings.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 affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/js/template.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 affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/js/todolist.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 affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/vendors/css/vendor.bundle.base.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 affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.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 affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/vendors/js/vendor.bundle.base.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 affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/public/admin/vendors/sweetalert/sweetalert.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 affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://calendar.ndbbank.com/robots.txt
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PL84FQZT
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe by injection issues, in which case there is still concern for browsers sniffing pages away from the actual content type. At "High" threshold this scan rule will not alert on client or server error respo

Instances	19
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it s 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 not perform MIME-sniffing at all, or that can be directed by the web application/web server to no 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	**Information Disclosure - Sensitive Information in URL**
Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI a most organizational compliance policies. You can configure the list of strings for this check to ad remove values specific to your environment.
URL	https://calendar.ndbbank.com/?_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	_token
Other Info	The URL contains potentially sensitive information. The following string was found via the patter token _token
Instances	1
Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10024

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matc made within script blocks or files are against the entire content not only comments.
URL	https://calendar.ndbbank.com/public/admin/js/todolist.js
Method	GET
Attack	
Evidence	todo
Other Info	The following pattern was used: \bTODO\b and was detected 4 times, the first in the element sta with: " var todoListItem = $('.todo-list');", see evidence field for the suspicious comment/snippet.
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js
Method	GET
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: " // If yo have a problem with this implementation, report a bug against the above spec", see evidence fie the suspicious comment/snippet.
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js

Method	GET
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 6 times, the first in the element starting with: " if (options && options.debug && window.console) {", see evidence field for the suspicious comment/snippet.
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 4 times, the first in the element sta with: " // Remove messages from rules, but allow them to be set separately", see evidence field the suspicious comment/snippet.
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: " // submits later.", see evidence field for the suspicious comment/snippet.
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 10 times, the first in the elemen starting with: " // Or option elements, check parent select in that case", see evidence field for the suspicious comment/snippet.
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js
Method	GET
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected in the element starting with: " // TO find a way to support input types date, datetime, datetime-local, month, time and week", see evidence field for the suspicious comment/snippet.
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 2 times, the first in the element sta with: " // - A user defined a `submitHandler`", see evidence field for the suspicious comment/snip
URL	https://calendar.ndbbank.com/public/admin/vendors/js/vendor.bundle.base.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "!func e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require ("popper.js")):"function"", see evidence field for the suspicious comment/snippet.

URL	https://calendar.ndbbank.com/public/admin/vendors/js/vendor.bundle.base.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!fu (t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==ty define&&define.amd?def", see evidence field for the suspicious comment/snippet.
URL	https://calendar.ndbbank.com/public/admin/vendors/js/vendor.bundle.base.js
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module. exports=e.document?t(e,!0):function(", see evidence field for the suspicious comment/snippet.
URL	https://calendar.ndbbank.com/public/admin/vendors/sweetalert/sweetalert.min.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "!func e){"object"==typeof exports&&"object"==typeof module?module.exports=e():"function"==typeof define&&define.amd?define", see evidence field for the suspicious comment/snippet.
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery-validate/1.19.3/jquery.validate.min.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!fu (a){"function"==typeof define&&define.amd?define(["jquery"],a):"object"==typeof module&&mod exports?module.exports=a", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PL84FQZT
Method	GET
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected 44 times, the first in the element start with: "function cb(a){for(var b=[],c=0;c<a.length();c++)a.has(c)&&(b[c]=a.get(c));return b};var db=function(){Ta.call(this)};za(db,Ta);", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PL84FQZT
Method	GET
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 3 times, the first in the element starting with: ""__googtag":{"logging":{"environments":"debug"},"access_globals":{"keys":[{"key": gtag","read":true,"write":true,"execute":true}", see evidence field for the suspicious comment/sni
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PL84FQZT
Method	GET
Attack	
Evidence	from

Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "if(c!= any"){try{if(c==="specific"&&g!=null&&lg(g,d))return}catch(h){throw e(f,{key:g},"Invalid key filter." throw e(f,{key:g", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PL84FQZT
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 11 times, the first in the element starting with: "case "port":f=String(Number(a.port)||(g==="http"?80:g==="https"?443:""));break;c "path":a.pathname||a.hostname||mb("TAGGING","", see evidence field for the suspicious comme /snippet.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PL84FQZT
Method	GET
Attack	
Evidence	SELECT
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "fu hc(a){var b;if(a instanceof $b)if(a instanceof $b)b=a.m;else throw Error("");else b=gc.test(a)?a:v return b};var j", see evidence field for the suspicious comment/snippet.
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 9 times, the first in the element st with: "<!-- <link rel="shortcut icon" href="https://calendar.ndbbank.com/public/admin/images/ndb png"> -->", see evidence field for the suspicious comment/snippet.
URL	https://calendar.ndbbank.com/?_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 9 times, the first in the element st with: "<!-- <link rel="shortcut icon" href="https://calendar.ndbbank.com/public/admin/images/ndb png"> -->", see evidence field for the suspicious comment/snippet.
Instances	20
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10027

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically the Ajax Spider may well be more effective than the standard one.
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
	<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start': new Date().getTime(),event:'gtm.js'})

Evidence	f=d.getElementsByTagName(s)[0], j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true; 'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f); })(window, document,'script','dataLayer','GTM-PL84FQZT');</script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern we application.
URL	https://calendar.ndbbank.com/? _token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start': new Date().getTime(),event:'gtm.js'}) f=d.getElementsByTagName(s)[0], j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true; 'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f); })(window, document,'script','dataLayer','GTM-PL84FQZT');</script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern we application.
Instances	2
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and pro to cache content. For static assets like css, js, or image files this might be intended, however, th resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://calendar.ndbbank.com/? _token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://calendar.ndbbank.com/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, mus revalidate". If an asset should be cached consider setting the directives "public, max-age, immu

Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	**Retrieved from Cache**
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://cdn.jsdelivr.net/jquery.validation/1.15.0/additional-methods.min.js
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery-validate/1.19.3/jquery.validate.min.js
Method	GET
Attack	
Evidence	Age: 1204
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery-validate/1.19.3/jquery.validate.min.js
Method	GET
Attack	
Evidence	Age: 1215
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/MaterialDesign-Webfont/3.0.39/css/materialdesignicons.min.css
Method	GET
Attack	
Evidence	Age: 1203
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/MaterialDesign-Webfont/3.0.39/css/materialdesignicons.min.css
Method	GET
Attack	
Evidence	Age: 1214
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.

Instances	5
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	
WASC Id	
Plugin Id	10050

Informational	**Session Management Response Identified**
Description	The given response has been identified as containing a session management token. The 'Other
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	eyJpdiI6IjR4VmpTd3lEd0g0T1lYcTBxU3NLaFE9PSIsInZhbHVlIjoiN3JnRnArb2xKd1dieDlQWVV
Other Info	cookie:ndb_session cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	eyJpdiI6IkNRQUFaRitsWFFpYVRUSnU2azFvTEE9PSIsInZhbHVlIjoieXBobUNiQXVGMTFjb2pl
Other Info	cookie:ndb_session cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	eyJpdiI6ImVkSUhKVUxBMGJ3TktwS0g3dEkvNWc9PSIsInZhbHVlIjoiMlFiTE9VMTZBTDQ0SVN
Other Info	cookie:ndb_session cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/
Method	GET
Attack	
Evidence	eyJpdiI6ImZpRGo2K092SzB6bjVVQU0rd21QK0E9PSIsInZhbHVlIjoiOEdBTDFSNHVka3Q2N2l
Other Info	cookie:ndb_session cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/
Method	GET

Attack	
Evidence	eyJpdiI6ImhiK3VGVEtxT0tKTWlZZ0pJK3RxL2c9PSIsInZhbHVlIjoiWjRTRW85MXFyY3prY244N
Other Info	cookie:ndb_session cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/?_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&
Method	GET
Attack	
Evidence	eyJpdiI6InV0MnVNWm1WcDRiR3NmWmE4OGlhbUE9PSIsInZhbHVlIjoiQkx4Qlp1bkExL3RtdG
Other Info	cookie:ndb_session cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/admin/images/background-desktop-img.jpg
Method	GET
Attack	
Evidence	eyJpdiI6ImZpRGo2K092SzB6bjVVQU0rd21QK0E9PSIsInZhbHVlIjoiOEdBTDFSNHVka3Q2N2l
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/admin/images/background-desktop-img.jpg
Method	GET
Attack	
Evidence	eyJpdiI6IlNmQzdXd2dZN09zRGJSQloxeTZmc3c9PSIsInZhbHVlIjoiQUg0VlR6NzRuQ1hvYy9aS
Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/favicon.ico
Method	GET
Attack	
Evidence	eyJpdiI6IkNRQUFaRitsWFFpYVRUSnU2azFvTEE9PSIsInZhbHVlIjoieXBobUNiQXVGMTFjb2pI
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/favicon.ico
Method	GET
Attack	
Evidence	eyJpdiI6ImhYdWJqZ01uYkU0OEhrTWxONVRzRVE9PSIsInZhbHVlIjoiUjdVMXRQNjBKQ0QzcK
Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/public/admin/css/vertical-layout-light
Method	GET
Attack	
Evidence	eyJpdiI6ImhiK3VGVEtxT0tKTWlZZ0pJK3RxL2c9PSIsInZhbHVlIjoiWjRTRW85MXFyY3prY244N
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/public/admin/css/vertical-layout-light
Method	GET
Attack	
Evidence	eyJpdiI6IkhUeGx3cnRiNUcxOTFRRnp0d2ZIVWc9PSIsInZhbHVlIjoiOTBWNkJXUWR1c3FJMXh

Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/public/admin/fonts/Roboto/Roboto-Light.woff2
Method	GET
Attack	
Evidence	eyJpdiI6ImZpRGo2K092SzB6bjVVQU0rd21QK0E9PSIsInZhbHVlIjoiOEdBTDFSNHVka3Q2N2l
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/public/admin/fonts/Roboto/Roboto-Light.woff2
Method	GET
Attack	
Evidence	eyJpdiI6IlNmQzdXd2dZN09zRGJSQloxeTZmc3c9PSIsInZhbHVlIjoiQUg0VlR6NzRuQ1hvYy9aS
Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/public/admin/fonts/Roboto/Roboto-Regular.woff2
Method	GET
Attack	
Evidence	eyJpdiI6IkNRQUFaRitsWFFpYVRUSnU2azFvTEE9PSIsInZhbHVlIjoieXBobUNiQXVGMTFjb2pl
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/public/admin/fonts/Roboto/Roboto-Regular.woff2
Method	GET
Attack	
Evidence	eyJpdiI6ImhYdWJqZ01uYkU0OEhrTWxONVRzRVE9PSIsInZhbHVlIjoiUjdVMXRQNjBKQ0Qzck
Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/public/admin/images
Method	GET
Attack	
Evidence	eyJpdiI6ImhiK3VGVEtxT0tKTWlZZ0pJK3RxL2c9PSIsInZhbHVlIjoiWjRTRW85MXFyY3prY244N
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/public/admin/images
Method	GET
Attack	
Evidence	eyJpdiI6IkhUeGx3cnRiNUcxOTFRRnp0d2ZIVWc9PSIsInZhbHVlIjoiOTBWNkJXUWR1c3FJMXh
Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/public/admin/images/ndb-logo.png
Method	GET
Attack	
Evidence	eyJpdiI6ImhiK3VGVEtxT0tKTWlZZ0pJK3RxL2c9PSIsInZhbHVlIjoiWjRTRW85MXFyY3prY244N
Other Info	cookie:ndb_session

URL	https://calendar.ndbbank.com/public/admin/images/ndb-logo.png
Method	GET
Attack	
Evidence	eyJpdiI6IkhUeGx3cnRiNUcxOTFRRnp0d2ZIVWc9PSIsInZhbHVlIjoiOTBWNkJXUWR1c3FJMXh
Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/public/admin/images/NDB-Logo_White.png
Method	GET
Attack	
Evidence	eyJpdiI6ImZpRGo2K092SzB6bjVVQU0rd21QK0E9PSIsInZhbHVlIjoiOEdBTDFSNHVka3Q2N2l
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/public/admin/images/NDB-Logo_White.png
Method	GET
Attack	
Evidence	eyJpdiI6IlNmQzdXd2dZN09zRGJSQloxeTZmc3c9PSIsInZhbHVlIjoiQUg0VlR6NzRuQ1hvYy9aS
Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/public/admin/js/hoverable-collapse.js
Method	GET
Attack	
Evidence	eyJpdiI6IkNRQUFaRitsWFFpYVRUSnU2azFvTEE9PSIsInZhbHVlIjoieXBobUNiQXVGMTFjb2p
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/public/admin/js/hoverable-collapse.js
Method	GET
Attack	
Evidence	eyJpdiI6ImhYdWJqZ01uYkU0OEhrTWxONVRzRVE9PSIsInZhbHVlIjoiUjdVMXRQNjBKQ0Qzck
Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/public/admin/js/todolist.js
Method	GET
Attack	
Evidence	eyJpdiI6ImZpRGo2K092SzB6bjVVQU0rd21QK0E9PSIsInZhbHVlIjoiOEdBTDFSNHVka3Q2N2l
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/public/admin/js/todolist.js
Method	GET
Attack	
Evidence	eyJpdiI6IlNmQzdXd2dZN09zRGJSQloxeTZmc3c9PSIsInZhbHVlIjoiQUg0VlR6NzRuQ1hvYy9aS
Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation
Method	GET

Attack	
Evidence	eyJpdiI6ImhiK3VGVEtxT0tKTWlZZ0pJK3RxL2c9PSIsInZhbHVlIjoiWjRTRW85MXFyY3prY244N
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation
Method	GET
Attack	
Evidence	eyJpdiI6IkhUeGx3cnRiNUcxOTFRRnp0d2ZIVWc9PSIsInZhbHVlIjoiOTBWNkJXUWR1c3FJMXh
Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js
Method	GET
Attack	
Evidence	eyJpdiI6IjR4VmpTd3lEd0g0T1lYcTBxU3NLaFE9PSIsInZhbHVlIjoiN3JnRnArb2xKd1dieDlQWVV
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js
Method	GET
Attack	
Evidence	eyJpdiI6IkNRQUFaRitsWFFpYVRUSnU2azFvTEE9PSIsInZhbHVlIjoieXBobUNiQXVGMTFjb2pl
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js
Method	GET
Attack	
Evidence	eyJpdiI6ImhiK3VGVEtxT0tKTWlZZ0pJK3RxL2c9PSIsInZhbHVlIjoiWjRTRW85MXFyY3prY244N
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js
Method	GET
Attack	
Evidence	eyJpdiI6IkZWRmhjRkNMRlhaa1ZYOUZ5SDZGSWc9PSIsInZhbHVlIjoiUmdmdElBWGw3YVVK 3D
Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/public/admin/vendors/jquery-validation/jquery.validate.min.js
Method	GET
Attack	
Evidence	eyJpdiI6ImhYdWJqZ01uYkU0OEhrTWxONVRzRVE9PSIsInZhbHVlIjoiUjdVMXRQNjBKQ0Qzck
Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/public/admin/vendors/js
Method	GET
Attack	

Evidence	eyJpdiI6ImhiK3VGVEtxT0tKTWlZZ0pJK3RxL2c9PSIsInZhbHVlIjoiWjRTRW85MXFyY3prY244N
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/public/admin/vendors/js
Method	GET
Attack	
Evidence	eyJpdiI6IkhUeGx3cnRiNUcxOTFRRnp0d2ZIVWc9PSIsInZhbHVlIjoiOTBWNkJXUWR1c3FJMXh
Other Info	cookie:XSRF-TOKEN
URL	https://calendar.ndbbank.com/public/admin/vendors/js/vendor.bundle.base.js
Method	GET
Attack	
Evidence	eyJpdiI6IkNRQUFaRitsWFFpYVRUSnU2azFvTEE9PSIsInZhbHVlIjoieXBobUNiQXVGMTFjb2pI
Other Info	cookie:ndb_session
URL	https://calendar.ndbbank.com/public/admin/vendors/js/vendor.bundle.base.js
Method	GET
Attack	
Evidence	eyJpdiI6ImhYdWJqZ01uYkU0OEhrTWxONVRzRVE9PSIsInZhbHVlIjoiUjdVMXRQNjBKQ0QzcK
Other Info	cookie:XSRF-TOKEN
Instances	37
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112

Informational	User Agent Fuzzer
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	https://calendar.ndbbank.com/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/

Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/
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	https://calendar.ndbbank.com/
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	https://calendar.ndbbank.com/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://calendar.ndbbank.com/
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	https://calendar.ndbbank.com/
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	https://calendar.ndbbank.com/
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	12
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

Informational	**User Controllable HTML Element Attribute (Potential XSS)**
Description	This check looks at user-supplied input in query string parameters and POST data to identify wh certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cro site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://calendar.ndbbank.com/?_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://calendar.ndbbank.com/?_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS The user-controlled value was: rtkyohugicyzwhe1gu6kwwv4utveyafr5ism0gvs
URL	https://calendar.ndbbank.com/?_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe
Method	GET
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://calendar.ndbbank.com/?_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS&full_name=ZAP&phone_numbe appears to include user input in: a(n) [meta] tag [content] attribute The user input found was:

	_token=RTkYohuGicyZwHE1Gu6KwWV4utVEYAFr5iSm0gVS The user-controlled value was: rtkyohugicyzwhe1gu6kwwv4utveyafr5ism0gvs
Instances	2
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031