ZAP by Checkmarx Scanning Report

Sites: https://content-signature-2.cdn.mozilla.net https://firefox-settings-attachments.cdn.mozilla.net https://firefox.settings.services.mozilla.com https://www.gravatar.com https://c.clarity.ms https://api.mastersunion.in https://cdn.filestackcontent.com https://fonts.gstatic.com https://scripts.clarity.ms https://www.clarity.ms https://stats.g.doubleclick.net https://analytics.google.com https://www.google.co.in https://www.googletagmanager.com https://fonts.googleapis.com https://unpkg.com https://admin.mastersunion.in https://l.clarity.ms https://ads.mozilla.org

Generated on Sat, 13 Sept 2025 00:17:36

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	4
Low	10
Informational	7

Alerts

Name	Risk Level	Number of Instances
SQL Injection - SQLite (Time Based)	High	1
Content Security Policy (CSP) Header Not Set	Medium	2
Cross-Domain Misconfiguration	Medium	40
Missing Anti-clickjacking Header	Medium	1
Session ID in URL Rewrite	Medium	7
Cookie No HttpOnly Flag	Low	60
Cookie Without Secure Flag	Low	30
Cookie with SameSite Attribute None	Low	31
Cookie without SameSite Attribute	Low	30
Cross-Domain JavaScript Source File Inclusion	Low	1
Private IP Disclosure	Low	2
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	25

Strict-Transport-Security Header Not Set	Low	40
Timestamp Disclosure - Unix	Low	58
X-Content-Type-Options Header Missing	Low	31
Authentication Request Identified	Informational	1
Information Disclosure - Suspicious Comments	Informational	17
Modern Web Application	Informational	1
Re-examine Cache-control Directives	Informational	23
Retrieved from Cache	Informational	23
Session Management Response Identified	Informational	31
User Agent Fuzzer	Informational	12

Alert Detail

High	SQL Injection - SQLite (Time Based)
Description	SQL injection may be possible.
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	GET
Attack	case randomblob(100000) when not null then 1 else 1 end
Evidence	
Other Info	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [615] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1,260] milliseconds, when the original unmodified query with value [10] took [124] milliseconds.
Instances	1
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.

Reference	html
CWE Id	89
WASC Id	19
Plugin Id	40024

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	https://admin.mastersunion.in/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://api.mastersunion.in/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	https://api.mastersunion.in
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other	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

Info	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://api.mastersunion.in/
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://api.mastersunion.in/api
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://api.mastersunion.in/api/v1
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://api.mastersunion.in/api/v1/auth
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://api.mastersunion.in/api/v1/auth/get-google-credentials
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://api.mastersunion.in/api/v1/auth/getGoogleApiData
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://api.mastersunion.in/api/v1/auth/login
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://api.mastersunion.in/api/v1/organization
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://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e
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://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard
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://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
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://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/courseMaster?searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
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://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/programMasterMain?searchParam=&pageSize=20&pageNo=1&filter=undefined
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://api.mastersunion.in/api/v1/organization/teacher
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://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
	The CORS misconfiguration on the web server permits cross-domain read requests from

Other Info	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://api.mastersunion.in/api/v1/users
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://api.mastersunion.in/api/v1/users/notification
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://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
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://api.mastersunion.in/favicon.ico
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.mastersunion.in/sitemap.xml
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other	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

Info	authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdn.filestackcontent.com/qkVt6g8rTtKSya5moY79
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://firefox.settings.services.mozilla.com/v1/
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://firefox.settings.services.mozilla.com/v1/buckets/main/collections/mfcdm-origins-list/changeset?_expected=1750871406038
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://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=mfcdm-origins-list&bucket=main&_expected=0
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://fonts.googleapis.com/css2?family=Inter:wght@400;500;600;700&family=Poppins:wght@400;500;600;700&family=Roboto:wght@400;500;700&display=swap&family=Public+Sans:wght@400;500;600;700
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
	The CORS misconfiguration on the web server permits cross-domain read requests from

Other Info	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://fonts.gstatic.com/s/inter/v20/UcC73FwrK3iLTeHuS_nVMrMxCp50SjIa1ZL7W0I5nvwU.woff2
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://fonts.gstatic.com/s/publicsans/v20/ijwRs572Xtc6ZYQws9YVwnNGfJ4.woff2
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://scripts.clarity.ms/0.8.30/clarity.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://unpkg.com/leaflet@1.7.1/dist/leaflet.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://unpkg.com/react-quill@1.3.3/dist/quill.snow.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser

Other Info	implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
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-PVRNXMJ
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://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	OPTIONS
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://api.mastersunion.in/api/v1/auth/login
Method	OPTIONS
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://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	OPTIONS
Attack	
Evidence	Access-Control-Allow-Origin: *
Other	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

Info	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://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/courseMaster?searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	OPTIONS
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://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/programMasterMain?searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	OPTIONS
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://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	OPTIONS
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://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	OPTIONS
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	40
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	Missing Anti-clickjacking Header
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://admin.mastersunion.in/
Method	GET
Attack	
Evidence	
Other Info	
Instances	1
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	Session ID in URL Rewrite
Description	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site ref
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59a1v9127094279za us&sr=1536x864&frm=0&pscdl=noapi&_s=1&tag_exp=101509157~103116026~103200004~10 mastersunion.in%2F&dt=Admin%20Panel%20Masters%27%20Union%3A%20Learn%20Busine
Method	POST
Attack	
Evidence	1757699261
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59a1v9127094279za us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEAAAAQ&tag_exp=101509157~103116026~103 mastersunion.in%2F&dt=Admin%20Panel%20Masters%27%20Union%3A%20Learn%20Busine
Method	POST
Attack	
Evidence	1757699261
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v912709427 us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEEAAAQ&_s=4&tag_exp=101509157~10311602 3A%2F%2Fadmin.mastersunion.in%2Flogin&dr=https%3A%2F%2Fadmin.mastersunion.in%2F first_field_id=email-login&ep.first_field_name=officialEmail&ep.first_field_type=officialEmail&epr

Method	POST
Attack	
Evidence	1757698965
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v912709427 us&sr=1536x864&frm=0&pscdl=noapi&_s=1&tag_exp=101509157~103116026~103200004~1 2Fadmin.mastersunion.in%2F&dt=Admin%20Panel%20Masters%27%20Union%3A%20Learn%
Method	POST
Attack	
Evidence	1757698965
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v912709427 us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEAAAAQ&_s=2&tag_exp=101509157~10311602 3A%2F%2Fadmin.mastersunion.in%2F&dt=Admin%20Panel%20Masters%27%20Union%3A%
Method	POST
Attack	
Evidence	1757698965
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v912709427 us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEAAAAQ&_s=3&tag_exp=101509157~10311602 mastersunion.in%2Flogin&dr=https%3A%2F%2Fadmin.mastersunion.in%2F&sid=1757698965
Method	POST
Attack	
Evidence	1757698965
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v912709427 us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEAAAAQ&_s=5&tag_exp=101509157~10311602 mastersunion.in%2F&dr=https%3A%2F%2Fadmin.mastersunion.in%2Flogin&sid=1757698965
Method	POST
Attack	
Evidence	1757698965
Other Info	
Instances	7
Solution	For secure content, put session ID in a cookie. To be even more secure consider using a combi
Reference	https://seclists.org/webappsec/2002/q4/111
CWE Id	598
WASC Id	13
Plugin Id	3

Low	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

URL	https://api.mastersunion.in
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1

Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/auth
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/get-google-credentials
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/get-google-credentials
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	GET
Attack	

Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard
Method	GET
Attack	

Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/courseMaster?searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/courseMaster?searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/programMasterMain?searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/programMasterMain?searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	

URL	https://api.mastersunion.in/api/v1/organization/teacher
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/users
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/users
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification

Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/favicon.ico
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/favicon.ico
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/robots.txt
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/robots.txt
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/sitemap.xml
Method	GET

Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/sitemap.xml
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	OPTIONS
Attack	

Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/courseMaster?searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/courseMaster?searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/programMasterMain?searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/programMasterMain?searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	

URL	https://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
Instances	60
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 via unencrypted connections.
URL	https://api.mastersunion.in
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB

Other Info	
URL	https://api.mastersunion.in/api
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/get-google-credentials
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	

URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/courseMaster?searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/programMasterMain?searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB

Other Info	
URL	https://api.mastersunion.in/api/v1/users
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/favicon.ico
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/robots.txt
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/sitemap.xml
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	

URL	https://api.mastersunion.in/api/v1/auth/login
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/courseMaster?searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/programMasterMain?searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
Other	

Info	
Instances	30
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	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
CWE Id	614
WASC Id	13
Plugin Id	10011

Low	**Cookie with SameSite Attribute None**
Description	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://api.mastersunion.in
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/auth
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	

URL	https://api.mastersunion.in/api/v1/auth/get-google-credentials
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	

URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/courseMaster?searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/programMasterMain?searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/users
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other	

Info	
URL	https://api.mastersunion.in/favicon.ico
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/robots.txt
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/sitemap.xml
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://www.clarity.ms/tag/on4tunsk4i?ref=gtm2
Method	GET
Attack	
Evidence	Set-Cookie: CLID
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	

URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/courseMaster?searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/programMasterMain?searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	
Evidence	Set-Cookie: AWSALBCORS
Other Info	
Instances	31
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://api.mastersunion.in
Method	GET

Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/get-google-credentials
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	GET
Attack	

Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/courseMaster?searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/programMasterMain?searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher
Method	GET

Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/users
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/favicon.ico
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/robots.txt
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/sitemap.xml
Method	GET
Attack	

Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/courseMaster?searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/programMasterMain?searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	OPTIONS
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	OPTIONS

Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
Other Info	
Instances	30
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://admin.mastersunion.in/
Method	GET
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H"></ /script>
Other Info	
Instances	1
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	**Private IP Disclosure**
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	https://admin.mastersunion.in/4105.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	10.4.6.2
Other Info	10.4.6.2
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET

Attack	
Evidence	192.168.0.0
Other Info	192.168.0.0 192.168.0.1 192.168.0.3 192.168.0.1 192.168.0.34 192.168.24.1 192.168.0.1
Instances	2
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	https://tools.ietf.org/html/rfc1918
CWE Id	497
WASC Id	13
Plugin Id	2

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response head
URL	https://admin.mastersunion.in/
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/2657.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/4092.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/41.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/4105.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/4431.bundle.de3ea36869a8ef880b02.js

Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/5455.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/5979.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/7229.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/7896.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/7926.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/9651.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/9850.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	

Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/assets/output.xml
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://api.mastersunion.in/robots.txt
Method	GET
Attack	
Evidence	awselb/2.0
Other Info	
URL	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.m
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59a1v9127094279za us&sr=1536x864&frm=0&pscdl=noapi&_s=1&tag_exp=101509157~103116026~103200004~10 2F&dt=Admin%20Panel%20Masters%27%20Union%3A%20Learn%20Business%20by%20Run
Method	POST
Attack	
Evidence	Golfe2
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59a1v9127094279za us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEAAAAQ&tag_exp=101509157~103116026~103 mastersunion.in%2F&dt=Admin%20Panel%20Masters%27%20Union%3A%20Learn%20Busine
Method	POST
Attack	
Evidence	Golfe2
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v912709427 us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEEAAAQ&_s=4&tag_exp=101509157~10311602 2F%2Fadmin.mastersunion.in%2Flogin&dr=https%3A%2F%2Fadmin.mastersunion.in%2F&dt=

	login&ep.first_field_name=officialEmail&ep.first_field_type=officialEmail&epn.first_field_position
Method	POST
Attack	
Evidence	Golfe2
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v9127094279 us&sr=1536x864&frm=0&pscdl=noapi&_s=1&tag_exp=101509157~103116026~103200004~10 mastersunion.in%2F&dt=Admin%20Panel%20Masters%27%20Union%3A%20Learn%20Busine
Method	POST
Attack	
Evidence	Golfe2
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v9127094279 us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEAAAAQ&_s=2&tag_exp=101509157~10311602 2F%2Fadmin.mastersunion.in%2F&dt=Admin%20Panel%20Masters%27%20Union%3A%20Le
Method	POST
Attack	
Evidence	Golfe2
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v9127094279 us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEAAAAQ&_s=3&tag_exp=101509157~10311602 2Flogin&dr=https%3A%2F%2Fadmin.mastersunion.in%2F&sid=1757698965&sct=1&seg=1&dt=
Method	POST
Attack	
Evidence	Golfe2
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v9127094279 us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEAAAAQ&_s=5&tag_exp=101509157~10311602 2F&dr=https%3A%2F%2Fadmin.mastersunion.in%2Flogin&sid=1757698965&sct=1&seg=1&dt=
Method	POST
Attack	
Evidence	Golfe2
Other Info	
URL	https://stats.g.doubleclick.net/g/collect?v=2&tid=G-SYEZL8KB0H&cid=924724902. 1757698965&gtm=45je59b0h2v9127094279za200zd9127094279&aip=1&dma=0&gcd=13l3l3l3
Method	POST
Attack	
Evidence	Golfe2
Other Info	
Instances	25
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress th
	https://httpd.apache.org/docs/current/mod/core.html#servertokens

Reference	https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10036

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web serv
URL	https://admin.mastersunion.in/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/2657.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/4092.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/41.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/4105.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/4431.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/5455.bundle.de3ea36869a8ef880b02.js

Method	GET
Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/5979.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/7229.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/7896.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/7926.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/9651.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/9850.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/assets/output.xml
Method	GET

Attack	
Evidence	
Other Info	
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://api.mastersunion.in/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://cdn.filestackcontent.com/qkVt6g8rTtKSya5moY79
Method	GET
Attack	
Evidence	
Other Info	
URL	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.m
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4b3
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/60c
Method	GET
Attack	
Evidence	

Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/70a
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/70d
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ea4
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ed8
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/eea
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f56
Method	GET
Attack	
Evidence	
Other Info	
URL	https://fonts.gstatic.com/s/inter/v20/UcC73FwrK3iLTeHuS_nVMrMxCp50SjIa1ZL7W0I5nvwU.w
Method	GET
Attack	
Evidence	
Other Info	

URL	https://fonts.gstatic.com/s/publicsans/v20/ijwRs572Xtc6ZYQws9YVwnNGfJ4.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://scripts.clarity.ms/0.8.30/clarity.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.clarity.ms/tag/on4tunsk4i?ref=gtm2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59a1v9127094279za us&sr=1536x864&frm=0&pscdl=noapi&_s=1&tag_exp=101509157~103116026~103200004~10 2F&dt=Admin%20Panel%20Masters%27%20Union%3A%20Learn%20Business%20by%20Rur
Method	POST
Attack	
Evidence	
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59a1v9127094279za us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEAAAAQ&tag_exp=101509157~103116026~103 mastersunion.in%2F&dt=Admin%20Panel%20Masters%27%20Union%3A%20Learn%20Busine
Method	POST
Attack	
Evidence	
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v912709427 us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEEAAAQ&_s=4&tag_exp=101509157~10311602 2F%2Fadmin.mastersunion.in%2Flogin&dr=https%3A%2F%2Fadmin.mastersunion.in%2F&dt= login&ep.first_field_name=officialEmail&ep.first_field_type=officialEmail&epn.first_field_position
Method	POST
Attack	
Evidence	
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v912709427 us&sr=1536x864&frm=0&pscdl=noapi&_s=1&tag_exp=101509157~103116026~103200004~10 mastersunion.in%2F&dt=Admin%20Panel%20Masters%27%20Union%3A%20Learn%20Busine
Method	POST

Attack	
Evidence	
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v9127094279 us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEAAAAQ&_s=2&tag_exp=101509157~10311602 2F%2Fadmin.mastersunion.in%2F&dt=Admin%20Panel%20Masters%27%20Union%3A%20Le
Method	POST
Attack	
Evidence	
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v9127094279 us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEAAAAQ&_s=3&tag_exp=101509157~10311602 2Flogin&dr=https%3A%2F%2Fadmin.mastersunion.in%2F&sid=1757698965&sct=1&seg=1&dt=
Method	POST
Attack	
Evidence	
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-SYEZL8KB0H&gtm=45je59b0h2v9127094279 us&sr=1536x864&frm=0&pscdl=noapi&_eu=AEAAAAQ&_s=5&tag_exp=101509157~10311602 2F&dr=https%3A%2F%2Fadmin.mastersunion.in%2Flogin&sid=1757698965&sct=1&seg=1&dt=
Method	POST
Attack	
Evidence	
Other Info	
URL	https://l.clarity.ms/collect
Method	POST
Attack	
Evidence	
Other Info	
URL	https://stats.g.doubleclick.net/g/collect?v=2&tid=G-SYEZL8KB0H&cid=924724902. 1757698965&gtm=45je59b0h2v9127094279za200zd9127094279&aip=1&dma=0&gcd=13l3l3l3
Method	POST
Attack	
Evidence	
Other Info	
Instances	40
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Stri
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	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1444681467
Other Info	1444681467, which evaluates to: 2015-10-13 01:54:27.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1473231341
Other Info	1473231341, which evaluates to: 2016-09-07 12:25:41.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1502002290
Other Info	1502002290, which evaluates to: 2017-08-06 12:21:30.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1530992060
Other Info	1530992060, which evaluates to: 2018-07-08 01:04:20.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1560198380
Other Info	1560198380, which evaluates to: 2019-06-11 01:56:20.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1700485571
Other Info	1700485571, which evaluates to: 2023-11-20 18:36:11.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET

Attack	
Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-26 06:53:13.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1732584194
Other Info	1732584194, which evaluates to: 2024-11-26 06:53:14.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1735328473
Other Info	1735328473, which evaluates to: 2024-12-28 01:11:13.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1770035416
Other Info	1770035416, which evaluates to: 2026-02-02 18:00:16.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1804603682
Other Info	1804603682, which evaluates to: 2027-03-09 20:18:02.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1839030562
Other Info	1839030562, which evaluates to: 2028-04-11 07:19:22.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1873313359
Other Info	1873313359, which evaluates to: 2029-05-13 02:19:19.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1894986606

Other Info	1894986606, which evaluates to: 2030-01-18 22:40:06.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1926607734
Other Info	1926607734, which evaluates to: 2031-01-19 22:18:54.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1958414417
Other Info	1958414417, which evaluates to: 2032-01-23 01:30:17.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	1990404162
Other Info	1990404162, which evaluates to: 2033-01-27 07:32:42.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	2022574463
Other Info	2022574463, which evaluates to: 2034-02-03 15:44:23.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	2054922799
Other Info	2054922799, which evaluates to: 2035-02-13 01:23:19.
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	GET
Attack	
Evidence	1743580800
Other Info	1743580800, which evaluates to: 2025-04-02 13:30:00.
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	GET
Attack	
Evidence	1748476800

Other Info	1748476800, which evaluates to: 2025-05-29 05:30:00.
URL	https://cdn.filestackcontent.com/qkVt6g8rTtKSya5moY79
Method	GET
Attack	
Evidence	1757696372
Other Info	1757696372, which evaluates to: 2025-09-12 22:29:32.
URL	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Method	GET
Attack	
Evidence	1703946492
Other Info	1703946492, which evaluates to: 2023-12-30 19:58:12.
URL	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Method	GET
Attack	
Evidence	1985046914
Other Info	1985046914, which evaluates to: 2032-11-26 07:25:14.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4b348bf3-00c5-4c6e-a945-e305c637ef09
Method	GET
Attack	
Evidence	1754961003
Other Info	1754961003, which evaluates to: 2025-08-12 06:40:03.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/60c396b3-efcb-4a00-85e1-f3f68055387e
Method	GET
Attack	
Evidence	1754961003
Other Info	1754961003, which evaluates to: 2025-08-12 06:40:03.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/70a56bff-9e7f-4364-92df-dddfb1fef1fe
Method	GET
Attack	
Evidence	1754961003
Other Info	1754961003, which evaluates to: 2025-08-12 06:40:03.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/70d35087-29a0-4d3a-971d-ac31f9349507
Method	GET
Attack	
Evidence	1754961003

Other Info	1754961003, which evaluates to: 2025-08-12 06:40:03.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ea414367-8661-4803-8ba2-344133af63f5
Method	GET
Attack	
Evidence	1754961003
Other Info	1754961003, which evaluates to: 2025-08-12 06:40:03.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ed87268d-8c74-40f5-b730-1ac808125445
Method	GET
Attack	
Evidence	1754961003
Other Info	1754961003, which evaluates to: 2025-08-12 06:40:03.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/eea64b17-b06a-4d0f-ba89-905cfadb6c70
Method	GET
Attack	
Evidence	1754961003
Other Info	1754961003, which evaluates to: 2025-08-12 06:40:03.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f56c8b62-79f9-4dd1-b08f-dd8844b13f50
Method	GET
Attack	
Evidence	1754961003
Other Info	1754961003, which evaluates to: 2025-08-12 06:40:03.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	1508970993
Other Info	1508970993, which evaluates to: 2017-10-26 04:06:33.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	1537002063
Other Info	1537002063, which evaluates to: 2018-09-15 14:31:03.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	

Evidence	1541459225
Other Info	1541459225, which evaluates to: 2018-11-06 04:37:05.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	1555081692
Other Info	1555081692, which evaluates to: 2019-04-12 20:38:12.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	1695183700
Other Info	1695183700, which evaluates to: 2023-09-20 09:51:40.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	1747873779
Other Info	1747873779, which evaluates to: 2025-05-22 05:59:39.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	1779033703
Other Info	1779033703, which evaluates to: 2026-05-17 21:31:43.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	1899447441
Other Info	1899447441, which evaluates to: 2030-03-11 13:47:21.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	1925078388
Other Info	1925078388, which evaluates to: 2031-01-02 05:29:48.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	1955562222
Other	

Info	1955562222, which evaluates to: 2031-12-21 01:13:42.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	1986661051
Other Info	1986661051, which evaluates to: 2032-12-14 23:47:31.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	1996064986
Other Info	1996064986, which evaluates to: 2033-04-02 19:59:46.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	2024104815
Other Info	2024104815, which evaluates to: 2034-02-21 08:50:15.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET
Attack	
Evidence	1508970993
Other Info	1508970993, which evaluates to: 2017-10-26 04:06:33.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET
Attack	
Evidence	1537002063
Other Info	1537002063, which evaluates to: 2018-09-15 14:31:03.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET
Attack	
Evidence	1541459225
Other Info	1541459225, which evaluates to: 2018-11-06 04:37:05.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET
Attack	
Evidence	1555081692
Other Info	1555081692, which evaluates to: 2019-04-12 20:38:12.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ

Method	GET
Attack	
Evidence	1695183700
Other Info	1695183700, which evaluates to: 2023-09-20 09:51:40.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET
Attack	
Evidence	1747873779
Other Info	1747873779, which evaluates to: 2025-05-22 05:59:39.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET
Attack	
Evidence	1779033703
Other Info	1779033703, which evaluates to: 2026-05-17 21:31:43.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET
Attack	
Evidence	1899447441
Other Info	1899447441, which evaluates to: 2030-03-11 13:47:21.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET
Attack	
Evidence	1925078388
Other Info	1925078388, which evaluates to: 2031-01-02 05:29:48.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET
Attack	
Evidence	1955562222
Other Info	1955562222, which evaluates to: 2031-12-21 01:13:42.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET
Attack	
Evidence	1986661051
Other Info	1986661051, which evaluates to: 2032-12-14 23:47:31.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET

Attack	
Evidence	1996064986
Other Info	1996064986, which evaluates to: 2033-04-02 19:59:46.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET
Attack	
Evidence	2024104815
Other Info	2024104815, which evaluates to: 2034-02-21 08:50:15.
Instances	58
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://admin.mastersunion.in/
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	https://admin.mastersunion.in/2657.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://admin.mastersunion.in/4092.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://admin.mastersunion.in/41.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://admin.mastersunion.in/4105.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://admin.mastersunion.in/4431.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://admin.mastersunion.in/5455.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://admin.mastersunion.in/5979.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://admin.mastersunion.in/7229.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://admin.mastersunion.in/7896.bundle.de3ea36869a8ef880b02.js

Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://admin.mastersunion.in/7926.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://admin.mastersunion.in/9651.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://admin.mastersunion.in/9850.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://admin.mastersunion.in/assets/output.xml
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	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2025-10-19-08-10-44.chain

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	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
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	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4b348bf3-00c5-4c6e-a945-e305c637ef09
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	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/60c396b3-efcb-4a00-85e1-f3f68055387e
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	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/70a56bff-9e7f-4364-92df-dddfb1fef1fe
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	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/70d35087-29a0-4d3a-971d-ac31f9349507
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	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ea414367-8661-4803-8ba2-344133af63f5
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	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ed87268d-8c74-40f5-b730-1ac808125445
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	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/eea64b17-b06a-4d0f-ba89-905cfadb6c70
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	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f56c8b62-79f9-4dd1-b08f-dd8844b13f50
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	https://scripts.clarity.ms/0.8.30/clarity.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://www.clarity.ms/tag/on4tunsk4i?ref=gtm2
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	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
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	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
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	https://ads.mozilla.org/v1/ads
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://l.clarity.ms/collect
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	31
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Authentication Request Identified**

Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	
Evidence	password
Other Info	userParam=officialEmail userValue=apresh.kumar@mastersunion.org passwordParam=password referer=https://admin.mastersunion.in/
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://admin.mastersunion.in/2657.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	Select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "// label=" Select Category"", see evidence field for the suspicious comment/snippet.
URL	https://admin.mastersunion.in/4092.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "/** * Removes all key-value entries from the list cache. * * @private * @name clear * @memberOf ListCache */", see evidence field for the suspicious comment/snippet.
URL	https://admin.mastersunion.in/41.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "// Play: Reset segments and continue playing full animation from current position", see evidence field for the suspicious comment/snippet.
URL	https://admin.mastersunion.in/4105.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected in likely comment: "// TODO: flags & (1<<11) // UTF8", see evidence field for the suspicious comment/snippet.
URL	https://admin.mastersunion.in/4431.bundle.de3ea36869a8ef880b02.js

Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "// import AnimateButton from 'components/@extended/AnimateButton';", see evidence field for the suspicious comment/snippet.
URL	https://admin.mastersunion.in/5455.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	Select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "// EXTERNAL MODULE: ./node_modules/@mui/material/Select/Select.js + 4 modules", see evidence field for the suspicious comment/snippet.
URL	https://admin.mastersunion.in/5979.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in likely comment: "// To avoid a bug when sets the Feb month", see evidence field for the suspicious comment/snippet.
URL	https://admin.mastersunion.in/7229.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//www.w3.org/2000/svg",svgWidth:0,svgHeight:0,noData:!1,locale:{},dom:{},memory:{methodsToExec:[]},shouldAnimate:!0,skipLastTime", see evidence field for the suspicious comment/snippet.
URL	https://admin.mastersunion.in/7896.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "// Initialize the object with the first column's value from args", see evidence field for the suspicious comment/snippet.
URL	https://admin.mastersunion.in/7926.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "// changes if the validation function is synchronous. It's different from", see evidence field for the suspicious comment/snippet.
URL	https://admin.mastersunion.in/9850.bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	from
Other	The following pattern was used: \bFROM\b and was detected in likely comment: "// import

Info	MainCard from 'components/MainCard';", see evidence field for the suspicious comment /snippet.
URL	https://admin.mastersunion.in/bundle.de3ea36869a8ef880b02.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "// `rgbToHsl`, `rgbToHsv`, `hslToRgb`, `hsvToRgb` modified from:", see evidence field for the suspicious comment/snippet.
URL	https://scripts.clarity.ms/0.8.30/clarity.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//"). concat("Electron");else{var r=u.drop;if(r&&r.length>0&&t&&t.indexOf("?")>0){var i=t.split("?"), o=i[0],c=i[1];a=o+"?"+c.spli", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//") &&(a=z.location.protocol+a);if(typeof URL==="function"){var c;a:{var d;try{d=new URL(a)} catch(w){c=void 0;break a}for(var e=", see evidence field for the suspicious comment /snippet.
URL	https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//") &&(a=z.location.protocol+a);if(typeof URL==="function"){var c;a:{var d;try{d=new URL(a)} catch(x){c=void 0;break a}for(var e=", see evidence field for the suspicious comment /snippet.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//") &&(a=z.location.protocol+a);if(typeof URL==="function"){var c;a:{var d;try{d=new URL(a)} catch(w){c=void 0;break a}for(var e=", see evidence field for the suspicious comment /snippet.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-PVRNXMJ
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//") &&(a=z.location.protocol+a);if(typeof URL==="function"){var c;a:{var d;try{d=new URL(a)} catch(x){c=void 0;break a}for(var e=", see evidence field for the suspicious comment /snippet.

Instances	17
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://admin.mastersunion.in/
Method	GET
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=G-SYEZL8KB0H"> /script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	1
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://admin.mastersunion.in/
Method	GET
Attack	
Evidence	max-age=0
Other Info	
URL	https://admin.mastersunion.in/assets/output.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://api.mastersunion.in
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://api.mastersunion.in/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/get-google-credentials
Method	GET
Attack	
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	GET
Attack	
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e
Method	GET
Attack	
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin-dashboard/?searchParam=
Method	GET
Attack	
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/courseMaster?searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	GET
Attack	
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/programMasterMain?searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	GET
Attack	
Evidence	

Other Info	
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	GET
Attack	
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4b348bf3-00c5-4c6e-a945-e305c637ef09
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/60c396b3-efcb-4a00-85e1-f3f68055387e
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/70a56bff-9e7f-4364-92df-dddfb1fef1fe
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/70d35087-29a0-4d3a-971d-ac31f9349507
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ea414367-8661-4803-8ba2-344133af63f5
Method	GET
Attack	

Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ed87268d-8c74-40f5-b730-1ac808125445
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/eea64b17-b06a-4d0f-ba89-905cfadb6c70
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f56c8b62-79f9-4dd1-b08f-dd8844b13f50
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox.settings.services.mozilla.com/v1/
Method	GET
Attack	
Evidence	max-age=3600
Other Info	
URL	https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/mfcdm-origins-list/changeset?_expected=1750871406038
Method	GET
Attack	
Evidence	max-age=3600
Other Info	
URL	https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=mfcdm-origins-list&bucket=main&_expected=0
Method	GET
Attack	
Evidence	max-age=3600
Other Info	
Instances	23

Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	**Retrieved from Cache**
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://admin.mastersunion.in/assets/output.xml
Method	GET
Attack	
Evidence	Hit from cloudfront
Other Info	
URL	https://cdn.filestackcontent.com/qkVt6g8rTtKSya5moY79
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4b348bf3-00c5-4c6e-a945-e305c637ef09
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/60c396b3-efcb-4a00-85e1-f3f68055387e
Method	GET
Attack	
Evidence	HIT

Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/70a56bff-9e7f-4364-92df-dddfb1fef1fe
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/70d35087-29a0-4d3a-971d-ac31f9349507
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ea414367-8661-4803-8ba2-344133af63f5
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ed87268d-8c74-40f5-b730-1ac808125445
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/eea64b17-b06a-4d0f-ba89-905cfadb6c70
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f56c8b62-79f9-4dd1-b08f-dd8844b13f50
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox.settings.services.mozilla.com/v1/
Method	GET

Attack	
Evidence	HIT
Other Info	
URL	https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/mfcdm-origins-list/changeset?_expected=1750871406038
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=mfcdm-origins-list&bucket=main&_expected=0
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2025-10-19-08-10-44.chain
Method	GET
Attack	
Evidence	Age: 1962
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://fonts.gstatic.com/s/inter/v20/UcC73FwrK3iLTeHuS_nVMrMxCp50SjIa1ZL7W0I5nvwU.woff2
Method	GET
Attack	
Evidence	Age: 174151
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://fonts.gstatic.com/s/inter/v20/UcC73FwrK3iLTeHuS_nVMrMxCp50SjIa1ZL7W0I5nvwU.woff2
Method	GET
Attack	
Evidence	Age: 174439
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://fonts.gstatic.com/s/publicsans/v20/ijwRs572Xtc6ZYQws9YVwnNGfJ4.woff2
Method	GET
Attack	
Evidence	Age: 119929
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://fonts.gstatic.com/s/publicsans/v20/ijwRs572Xtc6ZYQws9YVwnNGfJ4.woff2

Method	GET
Attack	
Evidence	Age: 123050
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://unpkg.com/leaflet@1.7.1/dist/leaflet.css
Method	GET
Attack	
Evidence	Age: 1193091
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://unpkg.com/leaflet@1.7.1/dist/leaflet.css
Method	GET
Attack	
Evidence	Age: 1193386
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://unpkg.com/react-quill@1.3.3/dist/quill.snow.css
Method	GET
Attack	
Evidence	Age: 289919
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://unpkg.com/react-quill@1.3.3/dist/quill.snow.css
Method	GET
Attack	
Evidence	Age: 290215
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	23
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	525
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 a set of header tokens that can be used in the Header Based Session Management Method. If t context which has a Session Management Method set to "Auto-Detect" then this rule will change management to use the tokens identified.
URL	https://api.mastersunion.in
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/auth
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/auth/get-google-credentials
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	GET
Attack	

Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/auth/login
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/organization
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin searchParam=
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/cours searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/progra searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	GET
Attack	

Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/organization/teacher
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion?termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/users
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/users/notification
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/robots.txt
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/sitemap.xml
Method	GET
Attack	
Evidence	AWSALBCORS

Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/auth/getGoogleApiData
Method	OPTIONS
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/auth/login
Method	OPTIONS
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/admin searchParam=
Method	OPTIONS
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/course searchParam=&pageSize=20&pageNo=1&draft=&courseTypeFilter=&courseTagFilter=
Method	OPTIONS
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/organization/77aa25d2-d52c-4c7b-ad4b-7b7de339fc4e/progra searchParam=&pageSize=20&pageNo=1&filter=undefined
Method	OPTIONS
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/organization/teacher/doubt-discussion? termCourseId=&programTermId=&sectionId=&pageNo=1&pageSize=10
Method	OPTIONS
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/users/notification/user-reach-out-notification
Method	OPTIONS
Attack	
Evidence	AWSALBCORS

Other Info	cookie:AWSALBCORS cookie:AWSALB
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS json:Data.token.refresh.token cookie:AWSALB json:Data.token.access.t
URL	https://api.mastersunion.in
Method	GET
Attack	
Evidence	AWSALBCORS
Other Info	cookie:AWSALBCORS
URL	https://c.clarity.ms/c.gif?ctsa=mr&CtsSyncId=A30B75CF09CA46EF8629AB5F0D3CAAAB&MUID=34D6223916A768D9
Method	POST
Attack	
Evidence	MUID
Other Info	cookie:MUID
Instances	31
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://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login

Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST

Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://api.mastersunion.in/api/v1/auth/login
Method	POST
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