ZAP Scanning Report

Generated on Mon, 8 Feb 2021 12:35:34

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	7
Informational	4

Alerts

Name	Risk Level	Number of Instances
Vulnerable JS Library	Medium	2
X-Frame-Options Header Not Set	Medium	4
Absence of Anti-CSRF Tokens	Low	19
Incomplete or No Cache-control and Pragma HTTP Header Set	Low	32
Private IP Disclosure	Low	8
X-Content-Type-Options Header Missing	Low	183
Information Disclosure - Suspicious Comments	Informational	28
Timestamp Disclosure - Unix	Informational	5802

Alert Detail

Vulnerable JS Library

Medium (Medium)

Description

The identified library jquery, version 3.4.1 is vulnerable.

- URL: http://localhost:3000/public/build/vendors~app.4d0490a94b199a11f40c.js
  - Method: `GET`
  - Evidence: `* jQuery JavaScript Library v3.4.1`
- URL: http://localhost:3000/public/build/angular~app.4d0490a94b199a11f40c.js
  - Method: `GET`
  - Evidence: `http://errors.angularjs.org/1.6.9/`

Instances: 2

Solution

Please upgrade to the latest version of jquery.

Other information

CVE-2020-11023

CVE-2020-11022

Reference

- https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
-

CWE Id : 829

Source ID : 3

X-Frame-Options Header Not Set

Medium (Medium)

Description

X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

- URL: http://localhost:3000/public/plugins/vonage-status-panel/module.html?v=1612698662038
  - Method: `GET`
  - Parameter: `X-Frame-Options`
- URL: http://localhost:3000/
  - Method: `GET`
  - Parameter: `X-Frame-Options`

Instances: 2

Solution

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (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. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).

Reference

- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

CWE Id : 16

WASC Id : 15

Source ID : 3

X-Frame-Options Header Not Set

Medium (Medium)

Description

X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

- URL: https://127.0.0.1:11000/docs
  - Method: `POST`
  - Parameter: `X-Frame-Options`
- URL: https://127.0.0.1:11000/
  - Method: `GET`
  - Parameter: `X-Frame-Options`

Instances: 2

Solution

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (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. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).

Reference

- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

CWE Id : 16

WASC Id : 15

Source ID : 3

Absence of Anti-CSRF Tokens

Low (Medium)

Description

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

* The victim has an active session on the target site.

* The victim is authenticated via HTTP auth on the target site.

* The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

- URL: http://localhost:3000/public/build/app.4d0490a94b199a11f40c.js
  - Method: `GET`
  - Evidence: `<form name=orgDetailsForm class=gf-form-group>`
- URL: http://localhost:3000/public/build/app.4d0490a94b199a11f40c.js
  - Method: `GET`
  - Evidence: `<form name=ctrl.saveForm ng-submit=ctrl.save() class="modal-content folder-modal" novalidate>`
- URL: http://localhost:3000/public/build/app.4d0490a94b199a11f40c.js
  - Method: `GET`
  - Evidence: `<form ng-if="mode === \'edit\' || mode === \'new\'" name=ctrl.form aria-label="Variable editor Form">`
- URL: http://localhost:3000/public/build/app.4d0490a94b199a11f40c.js
  - Method: `GET`
  - Evidence: `<form name=ctrl.saveForm ng-submit=ctrl.create() novalidate>`
- URL: http://localhost:3000/public/build/app.4d0490a94b199a11f40c.js
  - Method: `GET`
  - Evidence: `<form name=inviteForm class="login-form gf-form-group">`

Instances: 5

Solution

Phase: Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.

This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Other information

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF] was found in the following HTML form: [Form 1:].

Reference

- http://projects.webappsec.org/Cross-Site-Request-Forgery
- http://cwe.mitre.org/data/definitions/352.html

CWE Id : 352

WASC Id : 9

Source ID : 3

Absence of Anti-CSRF Tokens

Low (Medium)

Description

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

* The victim has an active session on the target site.

* The victim is authenticated via HTTP auth on the target site.

* The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form>`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form [ngFormOptions]="{updateOn: 'blur'}">`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form>`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form>`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form>`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form ngNativeValidate>`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form>`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form ngNativeValidate>`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form>`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form>`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form>`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form>`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form>`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Evidence: `<form>`

Instances: 14

Solution

Phase: Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.

This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Other information

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF] was found in the following HTML form: [Form 2:].

Reference

- http://projects.webappsec.org/Cross-Site-Request-Forgery
- http://cwe.mitre.org/data/definitions/352.html

CWE Id : 352

WASC Id : 9

Source ID : 3

Incomplete or No Cache-control and Pragma HTTP Header Set

Low (Medium)

Description

The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.

- URL: https://127.0.0.1:11000/docs/api.json
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/grafana/validation/z99hzWtmk
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/settings/alertmanager-api-host
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/user
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/cluster_conf/
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/settings/prometheus-api-host
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/cephfs
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/orchestrator/status
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/monitor
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/summary
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/auth/logout
  - Method: `POST`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/nfs-ganesha/status
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/feature_toggles
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/prometheus/rules
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/host
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/pool?stats=true
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/mgr/module/telemetry
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/ui-api/logging/js-error
  - Method: `POST`
  - Parameter: `Cache-Control`

- URL: https://127.0.0.1:11000/ui-api/standard_settings
  - Method: `GET`
  - Parameter: `Cache-Control`
- URL: https://127.0.0.1:11000/api/prometheus/notifications?from=last
  - Method: `GET`
  - Parameter: `Cache-Control`

Instances: 32

Solution

Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.

Reference

- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching

CWE Id : 525

WASC Id : 13

Source ID : 3

Private IP Disclosure

Low (Medium)

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: http://localhost:3000/api/datasources/proxy/6/api/v1/series?match%5B%5D=ceph_mon_metadata&start=1612695020&end=1612698620
  - Method: `GET`
  - Evidence: `172.20.0.6`

Instances: 1

Solution

Remove the private IP address from the HTTP response body. For comments, use JSP/ASP/PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.

Other information

172.20.0.6

172.20.0.6

172.20.0.6

172.20.0.2

172.20.0.2

172.20.0.2

Reference

- https://tools.ietf.org/html/rfc1918

CWE Id : 200

WASC Id : 13

Source ID : 3

Private IP Disclosure

Low (Medium)

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://127.0.0.1:11000/api/settings/prometheus-api-host
  - Method: `GET`
  - Evidence: `172.20.0.3:9090`
- URL: https://127.0.0.1:11000/api/settings/alertmanager-api-host
  - Method: `GET`
  - Evidence: `172.20.0.6:9093`
- URL: https://127.0.0.1:11000/swagger-ui-bundle.js
  - Method: `GET`
  - Evidence: `ip-172-31-21-173`
- URL: https://127.0.0.1:11000/api/monitor
  - Method: `GET`
  - Evidence: `172.20.0.2:10000`
- URL: https://127.0.0.1:11000/api/grafana/url
  - Method: `GET`
  - Evidence: `172.20.0.4:3000`
- URL: https://127.0.0.1:11000/api/health/minimal
  - Method: `GET`
  - Evidence: `172.20.0.2:6828`
- URL: https://127.0.0.1:11000/main.js
  - Method: `GET`
  - Evidence: `10.0.0.1:8080`

Instances: 7

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.

Other information

172.20.0.3:9090

Reference

- https://tools.ietf.org/html/rfc1918

CWE Id : 200

WASC Id : 13

Source ID : 3

X-Content-Type-Options Header Missing

Low (Medium)

Description

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query?query=sum%20((irate(node_disk_reads_completed%7Binstance%3D~%22(.*%22%7D%5B5m%5D)%20or%20irate(node_disk_reads_completed_total%7Binstance%3D~%22(.*%22%7D%5B5m%5D))%20%20%2B%20%0A(irate(node_disk_writes_completed%7Bins
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/series?match%5B%5D=ceph_health_status&start=1612677062&end=1612698662
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query?query=count(sum%20by%20(hostname)%20(ceph_osd_metadata))&time=1612698630
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: [http://localhost:3000/api/datasources/proxy/6/api/v1/query?query=avg%20(%0A%20%20label_replace((irate(node_disk_io_time_ms%5B5m%5D)%20%2F%2010%20)%20or%0A%20%20%20(irate(node_disk_io_time_seconds_total%5B5m%5D)%20*20100)%2C%20%22instance%22%2C%20%22%241%22%2C%20%22instance
  (http://localhost:3000/api/datasources/proxy/6/api/v1/query?query=avg%20(%0A%20%20label_replace((irate(node_disk_io_time_ms%5B5m%5D)%20%2F%2010%20)%20or%0A%20%20%20(irate(node_disk_io_time_seconds_total%5B5m%5D)%20*20100)%2C%20%22instance%22%2C%20%22%241%22%2C%20%22instance
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/public/build/DashboardPage.4d0490a94b199a11f40c.js
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/public/build/58.4d0490a94b199a11f40c.js
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: [http://localhost:3000/api/datasources/proxy/6/api/v1/query?query=avg(%0A%20%201%20-%20(%0A%20%20%20%20avg%20by(instance)%20%0A%20%20%20%20%20%20(irate(node_cpu_seconds_total%7Bmode%3D%27idle%27%2Cinstance%3D~%22(%7Ca%7Cb%7Cc%7C%7C8000%7C8002).*%22%7D%5B1m%5D)%20or%0A%20%20%20%20%20%20%
  (http://localhost:3000/api/datasources/proxy/6/api/v1/query?query=avg(%0A%20%201%20-%20(%0A%20%20%20%20avg%20by(instance)%20%0A%20%20%20%20%20%20(irate(node_cpu_seconds_total%7Bmode%3D%27idle%27%2Cinstance%3D~%22(%7Ca%7Cb%7Cc%7C%7C8000%7C8002).*%22%7D%5B1m%5D)%20or%0A%20%20%20%20%20%20%
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=sum(ceph_pg_active)&start=1612677060&end=1612698660&step=30
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=sum(irate(ceph_osd_recovery_ops%5B1m%5D))&start=1612677060&end=1612698660&step=20
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/api/annotations?dashboardId=1&from=1612677083457&to=1612698683457
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query?query=sum%20(%0A%20%20irate(node_network_receive_bytes%7Binstance%3D~%22(%7Cmon_hosts%7Cmds_hosts%7Crgw_hosts).*%22%2Cdevice!%3D%22lo%22%7D%5B1m%5D)%20or%0A%20%20irate(node_network_receive_bytes_total%7Binstance%3D~%2
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=sum(irate(ceph_osd_op_w_in_bytes%7Binstance%3D~%22ceph%3A9283%22%7D%5B1m%5D))&start=1612677080&end=1612698680&step=20
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/public/fonts/fontawesome-webfont.woff2?v=4.7.0
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=sum(ceph_pg_undersized)&start=1612677060&end=1612698660&step=30
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=ceph_osd_numpg%7Binstance%3D~%22ceph%3A9283%22%7D&start=1612677060&end=1612698660&step=60
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=quantile(0.95%2C%20ceph_osd_apply_latency_ms%7Binstance%3D~%22ceph%3A9283%22%7D)&start=1612677090&end=1612698690&step=30
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/public/build/grafanaPlugin.4d0490a94b199a11f40c.js
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=avg(ceph_osd_commit_latency_ms%7Binstance%3D~%22ceph%3A9283%22%7D)&start=1612677060&end=1612698660&step=30
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`

- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=quantile(0.95%2C%20ceph_osd_commit_latency_ms%7Binstance%3D~%22ceph%3A9283%22%7D)&start=1612677060&end=1612698660&step=30
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: http://localhost:3000/public/build/54.4d0490a94b199a11f40c.js
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`

Instances: 140

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.

Other information

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.

Reference

- http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
- https://owasp.org/www-community/Security_Headers

CWE Id : 16

WASC Id : 15

Source ID : 3

X-Content-Type-Options Header Missing

Low (Medium)

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://127.0.0.1:11000/swagger-ui.css
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/api/nfs-ganesha/status
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/api/summary
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/api/host
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/scripts.js
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/runtime.js
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/ui-api/langs
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/api/grafana/validation/z99hzWtmk
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/api/erasure_code_profile
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/ceph-pool-pool-module.js
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/api/health/minimal
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/main.js
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/api/settings/alertmanager-api-host
  - Method: `GET`
  - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/api/auth/check

    - Method: `POST`
    - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/api/settings/prometheus-api-host
    - Method: `GET`
    - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/docs/api.json
    - Method: `GET`
    - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/docs
    - Method: `POST`
    - Parameter: `X-Content-Type-Options`
- URL: https://127.0.0.1:11000/api/cluster_conf/mon_allow_pool_delete
    - Method: `GET`
    - Parameter: `X-Content-Type-Options`

Instances: 43

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.

Other information

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.

Reference

- http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
- https://owasp.org/www-community/Security_Headers

CWE Id : 16

WASC Id : 15

Source ID : 3

Information Disclosure - Suspicious Comments

Informational (Low)

Description

The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

- URL: http://localhost:3000/
    - Method: `GET`
- URL: http://localhost:3000/public/build/default~DashboardPage~SoloPanelPage~explore.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/default~DashboardPage~SoloPanelPage.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/50.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/60.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/grafanaPlugin.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/vendors~app.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/moment~app.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/59.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/DashboardPage.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/prometheusPlugin.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/49.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/brace.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/54.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/angular~app.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/app.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/55.4d0490a94b199a11f40c.js
    - Method: `GET`
- URL: http://localhost:3000/public/build/53.4d0490a94b199a11f40c.js
    - Method: `GET`

Instances: 18

Solution

Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

Other information

The following comment/snippet was identified via the pattern: \bUSER\b

Reference

-

CWE Id : 200

WASC Id : 13

Source ID : 3

Information Disclosure - Suspicious Comments

Informational (Low)

Description

The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

- URL: https://127.0.0.1:11000/scripts.js
  - Method: `GET`
- URL: https://127.0.0.1:11000/swagger-ui-bundle.js
  - Method: `GET`
- URL: https://127.0.0.1:11000/main.js
  - Method: `GET`
- URL: https://127.0.0.1:11000/styles.js
  - Method: `GET`
- URL: https://127.0.0.1:11000/vendor.js
  - Method: `GET`
- URL: https://127.0.0.1:11000/default~ceph-block-block-module~ceph-pool-pool-module.js
  - Method: `GET`
- URL: https://127.0.0.1:11000/polyfills.js
  - Method: `GET`
- URL: https://127.0.0.1:11000/ceph-pool-pool-module.js
  - Method: `GET`
- URL: https://127.0.0.1:11000/ceph-rgw-rgw-module.js
  - Method: `GET`
- URL: https://127.0.0.1:11000/runtime.js
  - Method: `GET`

Instances: 10

Solution

Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

Other information

The following comment/snippet was identified via the pattern: \bFROM\b

from = pair[1],

The following comment/snippet was identified via the pattern: \bFROM\b

convert[from] = convert[from] || {};

The following comment/snippet was identified via the pattern: \bFROM\b

convert[from][to] = convert[func] = (function(func) {

The following comment/snippet was identified via the pattern: \bFROM\b

from = this.convs[fspace];

The following comment/snippet was identified via the pattern: \bFROM\b

vals = convert[fspace][space](from);

The following comment/snippet was identified via the pattern: \bFROM\b

// YIQ equation from http://24ways.org/2010/calculating-color-contrast

The following comment/snippet was identified via the pattern: \bFROM\b

* Ported from sass implementation in C

The following comment/snippet was identified via the pattern: \bFROM\b

* Returns a unique id, sequentially generated from a global variable.

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bFROM\b

* Easing functions adapted from Robert Penner's easing equations.

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo handle `radius` as top-left, top-right, bottom-right, bottom-left array/object?

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo Support font.* options and renamed to toFont().

The following comment/snippet was identified via the pattern: \bUSER\b

onAnimationProgress: null, // user specified callback to fire on each step of the animation

The following comment/snippet was identified via the pattern: \bUSER\b

onAnimationComplete: null, // user specified callback to fire when the animation finishes

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bUSER\b

// This case happens when the user replaced the data array instance.

The following comment/snippet was identified via the pattern: \bUSER\b

// Re-sync meta data in case the user replaced the data array or if we missed

The following comment/snippet was identified via the pattern: \bFROM\b

// Boolean - Whether we animate scaling the Doughnut from the centre

The following comment/snippet was identified via the pattern: \bWHERE\b

// The rotation of the chart, where the first data arc begins.

The following comment/snippet was identified via the pattern: \bLATER\b

var startAngle = opts.rotation; // non reset case handled later

The following comment/snippet was identified via the pattern: \bLATER\b

var endAngle = opts.rotation; // non reset case handled later

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {Chart} chart - the chart to look at elements from

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {Chart} chart - the chart we are returning items from

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {Chart} chart - the chart we are returning items from

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {Chart} chart - the chart we are returning items from

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {Chart} chart - the chart we are returning items from

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {Chart} chart - the chart we are returning items from

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {Chart} chart - the chart we are returning items from

The following comment/snippet was identified via the pattern: \bWHERE\b

return helpers$1.where(array, function(v) {

The following comment/snippet was identified via the pattern: \bFROM\b

* @prop {number} weight - The weight used to sort the item. Higher weights are further away from the chart area

The following comment/snippet was identified via the pattern: \bFROM\b

* Remove a layoutItem from a chart

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {Chart} chart - the chart to remove the box from

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {ILayoutItem} layoutItem - the item to remove from the layout

The following comment/snippet was identified via the pattern: \bFROM\b

// Sort boxes by weight. A higher weight is further away from the chart area

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO re-limit horizontal axis height (this limit has affected only padding calculation since PR 1837)

The following comment/snippet was identified via the pattern: \bWHERE\b

* if the computed style is not expressed in pixels. That can happen in some cases where

The following comment/snippet was identified via the pattern: \bUSER\b

// which one can be specified by the user but also by charts as default option

The following comment/snippet was identified via the pattern: \bQUERY\b

// Let's keep track of this added resizer and thus avoid DOM query when removing it.

The following comment/snippet was identified via the pattern: \bSELECT\b

* Currently used by platform.js to select the proper implementation.

The following comment/snippet was identified via the pattern: \bFROM\b

// types from their toString() value but let's keep things flexible and assume it's

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

// @TODO Make possible to select another platform at build time.

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {*} item - The native item from which to acquire context (platform specific)

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {Chart} chart - Chart from which to listen for event

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {Chart} chart - Chart from which to remove the listener

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {function} listener - The listener function to remove from the event target.

The following comment/snippet was identified via the pattern: \bUSER\b

* but in some cases, this reference can be changed by the user when updating options.

The following comment/snippet was identified via the pattern: \bDB\b

// Scale registration object. Extensions can register new scale types (such as log or DB scales) and then

The following comment/snippet was identified via the pattern: \bFROM\b

* @returns {string[]} value if newline present - Returned from String split() method

The following comment/snippet was identified via the pattern: \bWHERE\b

// In the case where active.length === 0 we need to keep these at existing values for good animations

The following comment/snippet was identified via the pattern: \bUSER\b

// If the user provided a filter function, use it to modify the tooltip items

The following comment/snippet was identified via the pattern: \bUSER\b

// If the user provided a sorting function, use it to modify the tooltip items

The following comment/snippet was identified via the pattern: \bWHERE\b

// Point where the caret on the tooltip points to

The following comment/snippet was identified via the pattern: \bFROM\b

* the "instance" still need to be defined since it might be called from plugins.

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bFROM\b

console.error("Failed to create chart: can't acquire context from the given item");

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO(SB): I think we should be able to remove this custom case (options.scale)

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bWHERE\b

helpers$1.where = function(collection, filterCallback) {

The following comment/snippet was identified via the pattern: \bFROM\b

// Gets the angle from vertical upright to the point about a centre.

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bWHERE\b

// Implementation of the nice number algorithm used in determining where axis labels will go

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {any} value - the value to parse (usually comes from the data)

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bFROM\b

// and must not be accessed directly from outside this class. `this.ticks` being

The following comment/snippet was identified via the pattern: \bFROM\b

// IMPORTANT: from this point, we consider that `this.ticks` will NEVER change!

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO - improve this calculation

The following comment/snippet was identified via the pattern: \bFROM\b

me.paddingLeft = Math.max(paddingLeft - offsetLeft, 0) + 3; // add 3 px to move away from canvas edges

The following comment/snippet was identified via the pattern: \bFROM\b

* Used to get the data value from a given pixel. This is the inverse of getPixelForValue

The following comment/snippet was identified via the pattern: \bUSER\b

// user specified min value

The following comment/snippet was identified via the pattern: \bUSER\b

// user specified max value

The following comment/snippet was identified via the pattern: \bUSER\b

// If the user specified a precision, round to that number of decimal places

The following comment/snippet was identified via the pattern: \bUSER\b

// do nothing since that would make the chart weird. If the user really wants a weird chart

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO(v3): change this to positiveOrDefault

The following comment/snippet was identified via the pattern: \bFROM\b

// Boolean - Whether to animate scaling the chart from the centre

The following comment/snippet was identified via the pattern: \bWHERE\b

// Where it does, we store that angle and that index.

The following comment/snippet was identified via the pattern: \bFROM\b

// from the shape radius to move the point inwards by that x.

The following comment/snippet was identified via the pattern: \bFROM\b

// on each side, removing that from the size, halving it and adding the left x protrusion width.

The following comment/snippet was identified via the pattern: \bFROM\b

// Start from the top instead of right, so remove a quarter of the circle

The following comment/snippet was identified via the pattern: \bFROM\b

// Integer constants are from the ES6 spec.

The following comment/snippet was identified via the pattern: \bFROM\b

* @param {number[]} timestamps - timestamps sorted from lowest to highest.

The following comment/snippet was identified via the pattern: \bFROM\b

* If 'series', timestamps will be positioned at the same distance from each other. In this

The following comment/snippet was identified via the pattern: \bFROM\b

// @see adapted from https://www.anujgakhar.com/2014/03/01/binary-search-in-javascript/

The following comment/snippet was identified via the pattern: \bUSER\b

// The user might still use the deprecated `format` option for parsing.

The following comment/snippet was identified via the pattern: \bFROM\b

* Returns the start and end offsets from edges in the form of {start, end}

The following comment/snippet was identified via the pattern: \bWHERE\b

* where each value is a relative width to the scale and ranges between 0 and 1.

The following comment/snippet was identified via the pattern: \bFROM\b

* - 'series': data are spread at the same distance from each other.

The following comment/snippet was identified via the pattern: \bFROM\b

parser: false, // false == a pattern string from https://momentjs.com/docs/#/parsing/string-format/ or a custom callback that converts its argument to a moment

The following comment/snippet was identified via the pattern: \bFROM\b

format: false, // DEPRECATED false == date objects, moment object, callback or a pattern string from https://momentjs.com/docs/#/parsing/string-format/

The following comment/snippet was identified via the pattern: \bFROM\b

* - 'data': generates ticks from data (including labels from data {t|x|y} objects).

The following comment/snippet was identified via the pattern: \bUSER\b

* - 'labels': generates ticks from user given `data.labels` values ONLY.

The following comment/snippet was identified via the pattern: \bUSER\b

// Enforce limits with user min/max options

The following comment/snippet was identified via the pattern: \bFROM\b

function copyConfig(to, from) {

The following comment/snippet was identified via the pattern: \bFROM\b

if (!isUndefined(from._isAMomentObject)) {

The following comment/snippet was identified via the pattern: \bFROM\b

to._isAMomentObject = from._isAMomentObject;

The following comment/snippet was identified via the pattern: \bFROM\b

if (!isUndefined(from._i)) {

The following comment/snippet was identified via the pattern: \bFROM\b

to._i = from._i;

The following comment/snippet was identified via the pattern: \bFROM\b

if (!isUndefined(from._f)) {

The following comment/snippet was identified via the pattern: \bFROM\b

to._f = from._f;

The following comment/snippet was identified via the pattern: \bFROM\b

if (!isUndefined(from._l)) {

The following comment/snippet was identified via the pattern: \bFROM\b

to._l = from._l;

The following comment/snippet was identified via the pattern: \bFROM\b

if (!isUndefined(from._strict)) {

The following comment/snippet was identified via the pattern: \bFROM\b

to._strict = from._strict;

The following comment/snippet was identified via the pattern: \bFROM\b

if (!isUndefined(from._tzm)) {

The following comment/snippet was identified via the pattern: \bFROM\b

to._tzm = from._tzm;

The following comment/snippet was identified via the pattern: \bFROM\b

if (!isUndefined(from._isUTC)) {

The following comment/snippet was identified via the pattern: \bFROM\b

to._isUTC = from._isUTC;

The following comment/snippet was identified via the pattern: \bFROM\b

if (!isUndefined(from._offset)) {

The following comment/snippet was identified via the pattern: \bFROM\b

to._offset = from._offset;

The following comment/snippet was identified via the pattern: \bFROM\b

if (!isUndefined(from._pf)) {

The following comment/snippet was identified via the pattern: \bFROM\b

to._pf = getParsingFlags(from);

The following comment/snippet was identified via the pattern: \bFROM\b

if (!isUndefined(from._locale)) {

The following comment/snippet was identified via the pattern: \bFROM\b

to._locale = from._locale;

The following comment/snippet was identified via the pattern: \bFROM\b

val = from[prop];

The following comment/snippet was identified via the pattern: \bFROM\b

// number + (possibly) stuff coming from _dayOfMonthOrdinalParse.

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO: Remove "ordinalParse" fallback in next major release.

The following comment/snippet was identified via the pattern: \bFROM\b

// Code from http://stackoverflow.com/questions/3561493/is-there-a-regexp-escape-function-in-javascript

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO: add sorting

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO: Another silent failure?

The following comment/snippet was identified via the pattern: \bUSER\b

// Setting the hour should keep the time, because the user explicitly

The following comment/snippet was identified via the pattern: \bFROM\b

// pick the locale from the array

The following comment/snippet was identified via the pattern: \bFROM\b

// substring from most specific to least, but move to the next array item if it's a more specific variant than the current root

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO: Find a better way to register and load all the locales in Node

The following comment/snippet was identified via the pattern: \bUSER\b

//warn user if arguments are passed but the locale could not be set

The following comment/snippet was identified via the pattern: \bFROM\b

//compute day of the year from weeks and weekdays

The following comment/snippet was identified via the pattern: \bFROM\b

// Apply timezone offset from input. The actual utcOffset can be changed

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO: We need to take the current isoWeekYear, but that depends on

The following comment/snippet was identified via the pattern: \bFROM\b

// local weekday -- counting starts from beginning of week

The following comment/snippet was identified via the pattern: \bFROM\b

// date from iso format

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO: Replace the vanilla JS Date object with an indepentent day-of-week check.

The following comment/snippet was identified via the pattern: \bFROM\b

// date and time from ref 2822 format

The following comment/snippet was identified via the pattern: \bFROM\b

// date from iso format or fallback

The following comment/snippet was identified via the pattern: \bFROM\b

// date from string and format string

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO: Move this to another part of the creation flow to prevent circular deps

The following comment/snippet was identified via the pattern: \bFROM\b

// date from string and array of format strings

The following comment/snippet was identified via the pattern: \bFROM\b

// from milliseconds

The following comment/snippet was identified via the pattern: \bFROM\b

// Pick a moment m from moments so that m[fn](other) is true for all

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO: Use [].sort instead?

The following comment/snippet was identified via the pattern: \bFROM\b

// Because of dateAddRemove treats 24 hours as different from a

The following comment/snippet was identified via the pattern: \bFROM\b

// Return a moment from input, that is local/utc/zone equivalent to model.

The following comment/snippet was identified via the pattern: \bFROM\b

// from the actual represented time. That is why we call updateOffset

The following comment/snippet was identified via the pattern: \bFROM\b

// from http://docs.closure-library.googlecode.com/git/closure_goog_date_date.js.source.html

The following comment/snippet was identified via the pattern: \bFROM\b

} else if (typeof duration === 'object' && ('from' in duration || 'to' in duration)) {

The following comment/snippet was identified via the pattern: \bFROM\b

diffRes = momentsDifference(createLocal(duration.from), createLocal(duration.to));

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO: remove 'name' arg after deprecation is removed

The following comment/snippet was identified via the pattern: \bFROM\b

function isBetween (from, to, units, inclusivity) {

The following comment/snippet was identified via the pattern: \bFROM\b

var localFrom = isMoment(from) ? from : createLocal(from),

The following comment/snippet was identified via the pattern: \bFROM\b

function from (time, withoutSuffix) {

The following comment/snippet was identified via the pattern: \bFROM\b

return createDuration({to: this, from: time}).locale(this.locale()).humanize(!withoutSuffix);

The following comment/snippet was identified via the pattern: \bFROM\b

return this.from(createLocal(), withoutSuffix);

The following comment/snippet was identified via the pattern: \bFROM\b

return createDuration({from: this, to: time}).locale(this.locale()).humanize(!withoutSuffix);

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO: Remove "ordinalParse" fallback in next major release.

The following comment/snippet was identified via the pattern: \bFROM\b

proto.from = from;

The following comment/snippet was identified via the pattern: \bTODO\b

// TODO: Use this.as('ms')?

The following comment/snippet was identified via the pattern: \bFROM\b

// helper function for moment.fn.from, moment.fn.fromNow, and moment.duration.fn.humanize

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

// @todo if (fill[0] === '#')

The following comment/snippet was identified via the pattern: \bTODO\b

// @todo dispatch these helpers into appropriated helpers/helpers.* file and write unit tests!

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bFROM\b

* Provided for backward compatibility, inheriting from Chart.PlugingBase has no

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

The following comment/snippet was identified via the pattern: \bTODO\b

* @todo remove at version 3

Reference

-

CWE Id : 200

WASC Id : 13

Source ID : 3

Timestamp Disclosure - Unix

Informational (Low)

Description

A timestamp was disclosed by the application/web server - Unix

- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=avg(ceph_osd_apply_latency_ms%7Binstance%3D~%22ceph%3A9283%22%7D)&start=1612677060&end=1612698660&step=30
  - Method: `GET`
  - Evidence: `1612695360`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=sum(irate(ceph_osd_op_r_out_bytes%7Binstance%3D~%22ceph%3A9283%22%7D%5B1m%5D))&start=1612677060&end=1612698660&step=20
  - Method: `GET`
  - Evidence: `1612694560`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=sum(ceph_pg_total%20-%20ceph_pg_active)&start=1612677060&end=1612698660&step=30
  - Method: `GET`
  - Evidence: `1612698330`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=avg(ceph_osd_commit_latency_ms%7Binstance%3D~%22ceph%3A9283%22%7D)&start=1612677060&end=1612698660&step=30
  - Method: `GET`
  - Evidence: `1612694370`
- URL: [http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=topk(10%2C100%20*%20(%201%20-%20(%0A%20%20%20%20avg%20by(instance)%20%0A%20%20%20%20%20%20(irate(node_cpu_seconds_total%7Bmode%3D%27idle%27%2Cinstance%3D~%22(%7Ca%7Cb%7Cc%7C%7C8000%7C8002).*%22%7D%5B1m%5D)%20or%0A%20%20%20%20%20%20%20%20(http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=topk(10%2C100%20*%20(%201%20-%20(%0A%20%20%20%20avg%20by(instance)%20%0A%20%20%20%20%20%20(irate(node_cpu_seconds_total%7Bmode%3D%27idle%27%2Cinstance%3D~%22(%7Ca%7Cb%7Cc%7C%7C8000%7C8002). *%22%7D%5B1m%5D)%20or%0A%20%20%20%20%20%20%20%20%
  - Method: `GET`
  - Evidence: `1612695285`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=sum(irate(ceph_osd_op_r_out_bytes%7Binstance%3D~%22ceph%3A9283%22%7D%5B1m%5D))&start=1612677080&end=1612698680&step=20
  - Method: `GET`
  - Evidence: `1612695840`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=ceph_osd_stat_bytes_used%7Binstance%3D~%27ceph%3A9283%27%7D%20%2F%20ceph_osd_stat_bytes%7Binstance%3D~%27ceph%3A9283%27%7D&start=1612677060&end=1612698660&step=60
  - Method: `GET`
  - Evidence: `1612694760`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=sum(irate(ceph_osd_recovery_ops%5B1m%5D))&start=1612677060&end=1612698660&step=20
  - Method: `GET`
  - Evidence: `1612695760`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=sum(ceph_pg_total%20-%20ceph_pg_active)&start=1612677090&end=1612698690&step=30
  - Method: `GET`
  - Evidence: `1612695990`
- URL: [http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=topk(10%2C%20(sum%20by(instance)%20(%0A%20%20(%0A%20%20irate(node_network_receive_bytes%7Binstance%3D~%22(%7Ca%7Cb%7Cc%7C%7C8000%7C8002). *%22%2Cdevice!%3D%22lo%22%7D%5B1m%5D)%20or%0A%20%20irate(node_network (http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=topk(10%2C%20(sum%20by(instance)%20(%0A%20%20(%0A%20%20irate(node_network_receive_bytes%7Binstance%3D~%22(%7Ca%7Cb%7Cc%7C%7C8000%7C8002). *%22%2Cdevice!%3D%22lo%22%7D%5B1m%5D)%20or%0A%20%20irate(node_network
  - Method: `GET`
  - Evidence: `1612698600`
- URL: [http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=topk(10%2C%20(sum%20by(instance)%20(%0A%20%20(%0A%20%20irate(node_network_receive_bytes%7Binstance%3D~%22(%7Ca%7Cb%7Cc%7C%7C8000%7C8002). *%22%2Cdevice!%3D%22lo%22%7D%5B1m%5D)%20or%0A%20%20irate(node_network (http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=topk(10%2C%20(sum%20by(instance)%20(%0A%20%20(%0A%20%20irate(node_network_receive_bytes%7Binstance%3D~%22(%7Ca%7Cb%7Cc%7C%7C8000%7C8002). *%22%2Cdevice!%3D%22lo%22%7D%5B1m%5D)%20or%0A%20%20irate(node_network
  - Method: `GET`
  - Evidence: `1612695225`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=avg(ceph_osd_apply_latency_ms%7Binstance%3D~%22ceph%3A9283%22%7D)&start=1612677090&end=1612698690&step=30
  - Method: `GET`
  - Evidence: `1612698630`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=quantile(0.95%2C%20ceph_osd_apply_latency_ms%7Binstance%3D~%22ceph%3A9283%22%7D)&start=1612677090&end=1612698690&step=30
  - Method: `GET`
  - Evidence: `1612695030`

- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=sum(ceph_pg_total%20-%20ceph_pg_active)&start=1612677060&end=1612698660&step=30
  - Method: `GET`
  - Evidence: `1612696170`
- URL: [http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=topk(10%2C%20(sum%20by(instance)%20(%0A%20%20(%0A%20%20irate(node_network_receive_bytes%7Binstance%3D~%22(%7Ca%7Cb%7Cc%7C%7C8000%7C8002). *%22%2Cdevice!%3D%22lo%22%7D%5B1m%5D)%20or%0A%20%20irate(node_network*
(http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=topk(10%2C%20(sum%20by(instance)%20(%0A%20%20(%0A%20%20irate(node_network_receive_bytes%7Binstance%3D~%22(%7Ca%7Cb%7Cc%7C%7C8000%7C8002). *%22%2Cdevice!%3D%22lo%22%7D%5B1m%5D)%20or%0A%20%20irate(node_network*
  - Method: `GET`
  - Evidence: `1612698435`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=sum(irate(ceph_osd_op_w_in_bytes%7Binstance%3D~%22ceph%3A9283%22%7D%5B1m%5D))&start=1612677060&end=1612698660&step=20
  - Method: `GET`
  - Evidence: `1612694400`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=sum(ceph_pg_total%20-%20ceph_pg_active)&start=1612677090&end=1612698690&step=30
  - Method: `GET`
  - Evidence: `1612694310`
- URL: http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=sum(ceph_pg_active)&start=1612677060&end=1612698660&step=30
  - Method: `GET`
  - Evidence: `1612694370`
- URL: http://localhost:3000/public/build/vendors~app.4d0490a94b199a11f40c.js
  - Method: `GET`
  - Evidence: `16773077`
- URL: [http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=topk(10%2C100%20*%20(%201%20-*%20(%0A%20%20%20%20avg%20by(instance)%20%0A%20%20%20%20%20%20(irate(node_cpu_seconds_total%7Bmode%3D%27idle%27%2Cinstance%3D~%22(%7Ca%7Cb%7Cc%7C%7C8000%7C8002).%22%7D%5B1m%5D)%20or%0A%20%20%20%20%20%20%
(http://localhost:3000/api/datasources/proxy/6/api/v1/query_range?query=topk(10%2C100%20%20(%201%20-*%20(%0A%20%20%20%20avg%20by(instance)%20%0A%20%20%20%20%20%20(irate(node_cpu_seconds_total%7Bmode%3D%27idle%27%2Cinstance%3D~%22(%7Ca%7Cb%7Cc%7C%7C8000%7C8002). *%22%7D%5B1m%5D)%20or%0A%20%20%20%20%20%20%*
  - Method: `GET`
  - Evidence: `1612698180`

Instances: 3827

Solution

Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Other information

1612695360, which evaluates to: 2021-02-07 16:26:00

Reference

- http://projects.webappsec.org/w/page/13246936/Information%20Leakage

CWE Id : 200

WASC Id : 13

Source ID : 3

Timestamp Disclosure - Unix

Informational (Low)

Description

A timestamp was disclosed by the application/web server - Unix

- URL: https://127.0.0.1:11000/api/prometheus/rules
  - Method: `GET`
  - Evidence: `00075467`
- URL: https://127.0.0.1:11000/api/prometheus/rules
  - Method: `GET`
  - Evidence: `001341043`
- URL: https://127.0.0.1:11000/api/prometheus/rules
  - Method: `GET`
  - Evidence: `000308284`
- URL: https://127.0.0.1:11000/api/prometheus/rules
  - Method: `GET`
  - Evidence: `001132329`
- URL: https://127.0.0.1:11000/api/prometheus/rules
  - Method: `GET`
  - Evidence: `000530366`
- URL: https://127.0.0.1:11000/api/prometheus/rules
  - Method: `GET`
  - Evidence: `000381541`
- URL: https://127.0.0.1:11000/api/prometheus/rules
  - Method: `GET`
  - Evidence: `000662634`
- URL: https://127.0.0.1:11000/api/prometheus/rules
  - Method: `GET`
  - Evidence: `000117555`
- URL: https://127.0.0.1:11000/api/prometheus/rules
  - Method: `GET`
  - Evidence: `000286121`
- URL: https://127.0.0.1:11000/api/prometheus/rules
  - Method: `GET`
  - Evidence: `005972377`
- URL: https://127.0.0.1:11000/api/prometheus/rules

    - Method: `GET`
    - Evidence: `000581153`
- URL: https://127.0.0.1:11000/api/prometheus/rules
    - Method: `GET`
    - Evidence: `002061564`
- URL: https://127.0.0.1:11000/swagger-ui-bundle.js
    - Method: `GET`
    - Evidence: `858993459`
- URL: https://127.0.0.1:11000/api/prometheus/rules
    - Method: `GET`
    - Evidence: `000706153`
- URL: https://127.0.0.1:11000/api/prometheus/rules
    - Method: `GET`
    - Evidence: `003916639`
- URL: https://127.0.0.1:11000/api/prometheus/rules
    - Method: `GET`
    - Evidence: `00166513`
- URL: https://127.0.0.1:11000/api/prometheus/rules
    - Method: `GET`
    - Evidence: `000495785`
- URL: https://127.0.0.1:11000/vendor.js
    - Method: `GET`
    - Evidence: `143630929`
- URL: https://127.0.0.1:11000/swagger-ui-bundle.js
    - Method: `GET`
    - Evidence: `2003034995`
- URL: https://127.0.0.1:11000/api/prometheus/rules
    - Method: `GET`
    - Evidence: `000196197`

Instances: 1975

Solution

Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Other information

00075467, which evaluates to: 1970-01-02 02:27:47

Reference

- http://projects.webappsec.org/w/page/13246936/Information%20Leakage

CWE Id : 200

WASC Id : 13

Source ID : 3