netsparker

6/2/2023 8:40:22 PM (UTC+05:30)

Detailed Scan Report

https://github.com/Malshalmashi/Machine-learning-based-malware-detection

Scan Time	: 6/2/2023 8:39:42 PM (UTC+05:30)
Scan Duration	: 00:00:00:38
Total Requests	: 94
Average Speed	: 2.4r/s

Risk Level:
LOW

10
IDENTIFIED

2
CONFIRMED

0
CRITICAL

0
HIGH

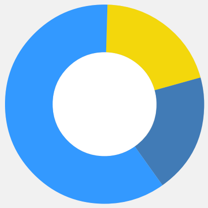
0
MEDIUM

2
LOW

2
BEST PRACTICE

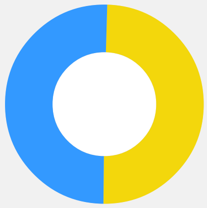
6
INFORMATION

Identified Vulnerabilities



🟥	Critical	0
🟧	High	0
🟧	Medium	0
🟨	Low	2
🟦	Best Practice	2
🟦	Information	6
	TOTAL	**10**

Confirmed Vulnerabilities



🟥	Critical	0
🟧	High	0
🟧	Medium	0
🟨	Low	1
🟦	Best Practice	0
🟦	Information	1
	TOTAL	**2**

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
⚑	[Possible] Phishing by Navigating Browser Tabs	GET	https://github.com/Malshalmashi/Machine-learning-based-malware-detection	
⚑	Cookie Not Marked as HttpOnly	GET	https://github.com/Malshalmashi/Machine-learning-based-malware-detection	
❗	Expect-CT Not Enabled	GET	https://github.com/Malshalmashi/Machine-learning-based-malware-detection	
❗	Subresource Integrity (SRI) Not Implemented	GET	https://github.com/Malshalmashi/Machine-learning-based-malware-detection	
ℹ	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://github.com/Malshalmashi/Machine-learning-based-malware-detection	
ℹ	data: Used in a Content Security Policy (CSP) Directive	GET	https://github.com/Malshalmashi/Machine-learning-based-malware-detection	
ℹ	Disabled X-XSS-Protection Header	GET	https://github.com/Malshalmashi/Machine-learning-based-malware-detection	
ℹ	Missing object-src in CSP Declaration	GET	https://github.com/Malshalmashi/Machine-learning-based-malware-detection	
ℹ	Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive	GET	https://github.com/Malshalmashi/Machine-learning-based-malware-detection	
ℹ	Cross-site Referrer Leakage through Referrer-Policy	GET	https://github.com/Malshalmashi/Machine-learning-based-malware-detection	

1. [Possible] Phishing by Navigating Browser Tabs

LOW ⚑ 1

Netsparker identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

Open windows with normal hrefs with the tag `target="_blank"`can modify *window.opener.location*and replace the parent webpage with something else, even on a different origin.

Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack `rel="noopener noreferrer"`attribute, a third party site can change the URL of the source tab using *window.opener.location.assign*and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

Vulnerabilities

1.1. https://github.com/MalshaImashi/Machine-learning-based-malware-detection

External Links

- https://github.blog

Certainty

Request

```
GET /MalshaImashi/Machine-learning-based-malware-detection HTTP/1.1
Host: github.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1244.7307 **Total Bytes Received :** 196804 **Body Length :** 193400 **Is Compressed :** No

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
ETag: W/"81e9554ee815e81ea2c816ffcef95e9c"
X-GitHub-Request-Id: CD12:0793:1011F26:11512CC:647A0639
Set-Cookie: _gh_sess=MzcJxePKrYiNzjL4nPNxXRKZVk4KvycnGkQaIldMsT%2BhiF403%2F16IrmG%2Bi1zH2G6HrIJnEFbmWMX
fLkY0mYRbKtdd6EIxnUP5rOTy%2B7fRP7cRm7vRifgw90mAMhrgRnstw3C3qeyu74WRgtGg%2FJtcbFc5CBMS4cltVnaFLhR1Lo4%2B
JJZa7lX4JGV5l1HFkxhcQogPcJr9IbAJL7VOmfxk%2FwS35JQUPXz9jm5XJKJz5KqUeRwDdUAbFmzLrE3OF5WoGYHlTUVZidhoReoYj
xa7w%3D%3D--CI38oZHfAAy5iGRj--kSd4OcXzede2olBI64b9dQ%3D%3D; Path=/; HttpOnly; Secure; SameSite=Lax
Set-Cookie: _octo=GH1.1.738414175.1685718585; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:0
9:45 GMT; Secure; SameSite=Lax
Set-Cookie: logged_in=no; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:09:45 GMT; HttpOnly; S
ecure; SameSite=Lax
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: GitHub.com
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Accept-Ranges: bytes
Referrer-Policy: no-referrer-when-downgrade
X-Frame-Options: deny
Vary: X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame, Accept-Encoding, Accept, X-Requested-With
Content-Type: text/html; charset=utf-8
Content-Security-Policy: default-src 'none'; base-uri 'self'; block-all-mixed-content; child-src githu
b.com/assets-cdn/worker/ gist.github.com/assets-cdn/worker/; connect-src 'self' uploads.github.com obje
cts-origin.githubusercontent.com www.githubstatus.com collector.github.com raw.githubusercontent.com ap
i.github.com github-cloud.s3.amazonaws.com github-production-repository-file-5c1aeb.s3.amazonaws.com gi
thub-production-upload-manifest-file-7fdce7.s3.amazonaws.com github-production-user-asset-6210df.s3.ama
zonaws.com cdn.optimizely.com logx.optimizely.com/v1/events *.actions.githubusercontent.com productionr
esultssa0.blob.core.windows.net/ productionresultssa1.blob.core.windows.net/ productionresultssa2.blob.
core.windows.net/ productionresultssa3.blob.core.windows.net/ productionresultssa4.blob.core.windows.ne
t/ wss://*.actions.githubusercontent.com github-production-repository-image-32fea6.s3.amazonaws.com git
hub-production-release-asset-2e65be.s3.amazonaws.com insights.github.com wss://alive.github.com; font-s
rc github.githubassets.com; form-action 'self' github.com gist.github.com objects-origin.githubusercont
ent.com; frame-ancestors 'none'; frame-src viewscreen.githubusercontent.com notebooks.githubuserconten
t.com; img-src 'self' data: github.githubassets.com media.githubusercontent.com camo.githubusercontent.
com identicons.github.com avatars.githubusercontent.com github-cloud.s3.amazonaws.com objects.githubuse
rcontent.com objects-origin.githubusercontent.com secured-user-images.githubusercontent.com/ user-image
s.githubusercontent.com/ private-user-images.githubusercontent.com opengraph.githubassets.com github-pr
oduction-user-asset-6210df.s3.amazonaws.com customer-stories-feed.github.com spotlights-feed.github.com
 *.githubusercontent.com; manifest-src 'self'; media-src github.com user-images.githubusercontent.com/
 secured-user-images.githubusercontent.com/ private-user-images.githubusercontent.com; script-src githu
b.githubassets.com; style-src 'unsafe-inline' github.githubassets.com; worker-src github.com/assets-cd
n/worker/ gist.github.com/assets-cdn/worker/
Date: Fri, 02
…
k" data-analytics-event="{&quot;category&quot;:&quot;Header dropdown (logged out), Product&quot;,&quot;
action&quot;:&quot;click to go to Blog&quot;,&quot;label&quot;:&quot;ref_cta:Blog;&quot;}" href="http
```

```
s://github.blog">
Blog

<svg aria-hidden="true" height="16" viewBox="0 0 16 16" version="1.1" width="16" data-view-component="t
rue" class="octicon octicon-link-external HeaderMenu-external-icon color-fg-su
…
ent="{&quot;category&quot;:&quot;Footer&quot;,&quot;action&quot;:&quot;go to training&quot;,&quot;label
&quot;:&quot;text:training&quot;}">Training</a></li>
<li class="mr-3 mr-lg-0"><a href="https://github.blog" data-analytics-event="{&quot;category&quot;:&quo
t;Footer&quot;,&quot;action&quot;:&quot;go to blog&quot;,&quot;label&quot;:&quot;text:blog&quot;}">Blog
</a></li>
<li><a data-ga-click="Foote
…
```

Remedy

- Add `rel=noopener`to the linksto prevent pages from abusing *window.opener*. This ensures that the page cannot access the *window.opener*property in Chrome and Opera browsers.

- For older browsers and in Firefox, you can add `rel=noreferrer`which additionally disables the Referer header.

```
<a href="..." target="_blank" rel="noopener noreferrer">...</a>
```

External References

- [Reverse Tabnabbing]
- [Blankshield & Reverse Tabnabbing Attacks]
- [Target="_blank" - the most underestimated vulnerability ever]

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

2. Cookie Not Marked as HttpOnly

LOW 1 CONFIRMED 1

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Vulnerabilities

2.1. https://github.com/MalshaImashi/Machine-learning-based-malware-detection

CONFIRMED

Identified Cookie(s)

- _octo

Cookie Source

- HTTP Header

Request

```
GET /MalshaImashi/Machine-learning-based-malware-detection HTTP/1.1
Host: github.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1244.7307 **Total Bytes Received :** 196804 **Body Length :** 193400 **Is Compressed :** No

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
ETag: W/"81e9554ee815e81ea2c816ffcef95e9c"
X-GitHub-Request-Id: CD12:0793:1011F26:11512CC:647A0639
Set-Cookie: _gh_sess=MzcJxePKrYiNzjL4nPNxXRKZVk4KvycnGkQaIldMsT%2BhiF403%2F16IrmG%2Bi1zH2G6HrIJnEFbmWMX
fLkY0mYRbKtdd6EIxnUP5rOTy%2B7fRP7cRm7vRifgw90mAMhrgRnstw3C3qeyu74WRgtGg%2FJtcbFc5CBMS4cltVnaFLhR1Lo4%2B
JJZa7lX4JGV5l1HFkxhcQogPcJr9IbAJL7VOmfxk%2FwS35JQUPXz9jm5XJKJz5KqUeRwDdUAbFmzLrE3OF5WoGYHlTUVZidhoReoYj
xa7w%3D%3D--CI38oZHfAAy5iGRj--kSd4OcXzede2olBI64b9dQ%3D%3D; Path=/; HttpOnly; Secure; SameSite=Lax
Set-Cookie: _octo=GH1.1.738414175.1685718585; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:0
9:45 GMT; Secure; SameSite=Lax
Set-Cookie: logged_in=no; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:09:45 GMT; HttpOnly; S
ecure; SameSite=Lax
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: GitHub.com
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Accept-Ranges: bytes
Referrer-Policy: no-referrer-when-downgrade
X-Frame-Options: deny
Vary: X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame, Accept-Encoding, Accept, X-Requested-With
Content-Type: text/html; charset=utf-8
Content-Security-Policy: default-src 'none'; base-uri 'self'; block-all-mixed-content; child-src githu
b.com/assets-cdn/worker/ gist.github.com/assets-cdn/worker/; connect-src 'self' uploads.github.com obje
cts-origin.githubusercontent.com www.githubstatus.com collector.github.com raw.githubusercontent.com ap
i.github.com github-cloud.s3.amazonaws.com github-production-repository-file-5c1aeb.s3.amazonaws.com gi
thub-production-upload-manifest-file-7fdce7.s3.amazonaws.com github-production-user-asset-6210df.s3.ama
zonaws.com cdn.optimizely.com logx.optimizely.com/v1/events *.actions.githubusercontent.com productionr
esultssa0.blob.core.windows.net/ productionresultssa1.blob.core.windows.net/ productionresultssa2.blob.
core.windows.net/ productionresultssa3.blob.core.windows.net/ productionresultssa4.blob.core.windows.ne
t/ wss://*.actions.githubusercontent.com github-production-repository-image-32fea6.s3.amazonaws.com git
hub-production-release-asset-2e65be.s3.amazonaws.com insights.github.com wss://alive.github.com; font-s
rc github.githubassets.com; form-action 'self' github.com gist.github.com objects-origin.githubusercont
ent.com; frame-ancestors 'none'; frame-src viewscreen.githubusercontent.com notebooks.githubuserconten
t.com; img-src 'self' data: github.githubassets.com media.githubusercontent.com camo.githubusercontent.
com identicons.github.com avatars.githubusercontent.com github-cloud.s3.amazonaws.com objects.githubuse
rcontent.com objects-origin.githubusercontent.com secured-user-images.githubusercontent.com/ user-image
s.githubusercontent.com/ private-user-images.githubusercontent.com opengraph.githubassets.com github-pr
oduction-user-asset-6210df.s3.amazonaws.com customer-stories-feed.github.com spotlights-feed.github.com
 *.githubusercontent.com; manifest-src 'self'; media-src github.com user-images.githubusercontent.com/
 secured-user-images.githubusercontent.com/ private-user-images.githubusercontent.com; script-src githu
b.githubassets.com; style-src 'unsafe-inline' github.githubassets.com; worker-src github.com/assets-cd
n/worker/ gist.github.com/assets-cdn/worker/
Date: Fri, 02
…
a7lX4JGV5l1HFkxhcQogPcJr9IbAJL7VOmfxk%2FwS35JQUPXz9jm5XJKJz5KqUeRwDdUAbFmzLrE3OF5WoGYHlTUVZidhoReoYjxa7
w%3D%3D--CI38oZHfAAy5iGRj--kSd4OcXzede2olBI64b9dQ%3D%3D; Path=/; HttpOnly; Secure; SameSite=Lax
```

```
Set-Cookie: _octo=GH1.1.738414175.1685718585; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:0
9:45 GMT; Secure; SameSite=Lax

Set-Cookie: logged_in=no; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:09:45 GMT; HttpOnly; S
ecure; SameSite=Lax
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Tr
…
```

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnelto bypass HTTPOnly protection.

External References

- Netsparker - Security Cookies - HTTPOnly Flag
- OWASP HTTPOnly Cookies
- MSDN - ASP.NET HTTPOnly Cookies

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
CAPEC	107
WASC	15
ISO27001	A.14.2.5

3. Expect-CT Not Enabled

BEST PRACTICE | **1**

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissused certificates to be used.

Vulnerabilities

3.1. https://github.com/MalshaImashi/Machine-learning-based-malware-detection

Certainty

Request

```
GET /MalshaImashi/Machine-learning-based-malware-detection HTTP/1.1
Host: github.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1244.7307 **Total Bytes Received :** 196804 **Body Length :** 193400 **Is Compressed :** No

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
ETag: W/"81e9554ee815e81ea2c816ffcef95e9c"
X-GitHub-Request-Id: CD12:0793:1011F26:11512CC:647A0639
Set-Cookie: _gh_sess=MzcJxePKrYiNzjL4nPNxXRKZVk4KvycnGkQaIldMsT%2BhiF403%2F16IrmG%2Bi1zH2G6HrIJnEFbmWMX
fLkY0mYRbKtdd6EIxnUP5rOTy%2B7fRP7cRm7vRifgw90mAMhrgRnstw3C3qeyu74WRgtGg%2FJtcbFc5CBMS4cltVnaFLhR1Lo4%2B
JJZa7lX4JGV5l1HFkxhcQogPcJr9IbAJL7VOmfxk%2FwS35JQUPXz9jm5XJKJz5KqUeRwDdUAbFmzLrE3OF5WoGYHlTUVZidhoReoYj
xa7w%3D%3D--CI38oZHfAAy5iGRj--kSd4OcXzede2olBI64b9dQ%3D%3D; Path=/; HttpOnly; Secure; SameSite=Lax
Set-Cookie: _octo=GH1.1.738414175.1685718585; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:0
9:45 GMT; Secure; SameSite=Lax
Set-Cookie: logged_in=no; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:09:45 GMT; HttpOnly; S
ecure; SameSite=Lax
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: GitHub.com
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Accept-Ranges: bytes
Referrer-Policy: no-referrer-when-downgrade
X-Frame-Options: deny
Vary: X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame, Accept-Encoding, Accept, X-Requested-With
Content-Type: text/html; charset=utf-8
Content-Security-Policy: default-src 'none'; base-uri 'self'; block-all-mixed-content; child-src githu
b.com/assets-cdn/worker/ gist.github.com/assets-cdn/worker/; connect-src 'self' uploads.github.com obje
cts-origin.githubusercontent.com www.githubstatus.com collector.github.com raw.githubusercontent.com ap
i.github.com github-cloud.s3.amazonaws.com github-production-repository-file-5c1aeb.s3.amazonaws.com gi
thub-production-upload-manifest-file-7fdce7.s3.amazonaws.com github-production-user-asset-6210df.s3.ama
zonaws.com cdn.optimizely.com logx.optimizely.com/v1/events *.actions.githubusercontent.com productionr
esultssa0.blob.core.windows.net/ productionresultssa1.blob.core.windows.net/ productionresultssa2.blob.
core.windows.net/ productionresultssa
…
```

Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode**first. If everything goes well and your certificate is ready, go with the Expect-CT enforcemode. To use **report-only mode**first, omit **enforce**flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

External References

- Expect-CT Extension for HTTP
- Expect-CT HTTP Header
- Expect-CT Header

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

4. Subresource Integrity (SRI) Not Implemented

BEST PRACTICE | 1

Subresource Integrity (SRI) provides a mechanism to check integrity of the resource hosted by third parties like Content Delivery Networks (CDNs) and verifies that the fetched resource has been delivered without unexpected manipulation.

SRI does this using hash comparison mechanism. In this way, hash value declared in HTML elements (for now only script and link elements are supported) will be compared with the hash value of the resource hosted by third party.

Use of SRI is recommended as a best-practice, whenever libraries are loaded from a third-party source.

Vulnerabilities

4.1. https://github.com/MalshaImashi/Machine-learning-based-malware-detection

Identified Sub Resource(s)

- https://github.githubassets.com/assets/light-0946cdc16f15.css
- https://github.githubassets.com/assets/dark-3946c959759a.css
- https://github.githubassets.com/assets/primer-primitives-fb1d51d1ef66.css
- https://github.githubassets.com/assets/primer-0e3420bbec16.css
- https://github.githubassets.com/assets/global-0d04dfcdc794.css
- https://github.githubassets.com/assets/github-c7a3a0ac71d4.css
- https://github.githubassets.com/assets/code-9271f811184f.css
- https://github.githubassets.com/assets/wp-runtime-14f3ad9684cf.js
- https://github.githubassets.com/assets/vendors-node_modules_stacktrace-parser_dist_stack-trace-parser_esm_js-node_modules_github_bro-a4c183-ae93d3fba59c.js
- https://github.githubassets.com/assets/ui_packages_failbot_failbot_ts-e38c93eab86e.js
- https://github.githubassets.com/assets/environment-de3997b81651.js
- https://github.githubassets.com/assets/vendors-node_modules_github_selector-observer_dist_index_esm_js-2646a2c533e3.js
- https://github.githubassets.com/assets/vendors-node_modules_github_relative-time-element_dist_index_js-99e288659d4f.js
- https://github.githubassets.com/assets/vendors-node_modules_fzy_js_index_js-node_modules_github_markdown-toolbar-element_dist_index_js-e3de700a4c9d.js
- https://github.githubassets.com/assets/vendors-node_modules_delegated-events_dist_index_js-node_modules_github_auto-complete-element-5b3870-ff38694180c6.js
- https://github.githubassets.com/assets/vendors-node_modules_github_file-attachment-element_dist_index_js-node_modules_github_text-ex-3415a8-7ecc10fb88d0.js
- https://github.githubassets.com/assets/vendors-node_modules_github_filter-input-element_dist_index_js-node_modules_github_remote-inp-8873b7-5771678648e0.js
- https://github.githubassets.com/assets/vendors-node_modules_primer_view-components_app_components_primer_primer_js-node_modules_gith-3af896-d8cf3e5f5813.js
- https://github.githubassets.com/assets/github-elements-6f05fe60d18a.js
- https://github.githubassets.com/assets/element-registry-84be4ef284ec.js
- https://github.githubassets.com/assets/vendors-node_modules_lit-html_lit-html_js-9d9fe1859ce5.js
- https://github.githubassets.com/assets/vendors-node_modules_github_mini-throttle_dist_index_js-node_modules_github_alive-client_dist-bf5aa2-424aa982deef.js
- https://github.githubassets.com/assets/vendors-node_modules_github_turbo_dist_turbo_es2017-esm_js-ba0e4d5b3207.js
- https://github.githubassets.com/assets/vendors-node_modules_color-convert_index_js-node_modules_github_jtml_lib_index_js-40bf234a19dc.js

- https://github.githubassets.com/assets/vendors-node_modules_github_remote-form_dist_index_js-node_modules_scroll-anchoring_dist_scro-52dc4b-e1e33bfc0b7e.js
- https://github.githubassets.com/assets/vendors-node_modules_github_paste-markdown_dist_index_esm_js-node_modules_github_quote-select-743f1d-1b20d530fbf0.js
- https://github.githubassets.com/assets/app_assets_modules_github_updatable-content_ts-dadb69f79923.js
- https://github.githubassets.com/assets/app_assets_modules_github_behaviors_keyboard-shortcuts-helper_ts-app_assets_modules_github_be-f5afdb-3f05df4c282b.js
- https://github.githubassets.com/assets/app_assets_modules_github_sticky-scroll-into-view_ts-050ad6637d58.js
- https://github.githubassets.com/assets/app_assets_modules_github_behaviors_ajax-error_ts-app_assets_modules_github_behaviors_include-2e2258-7effad8d88d4.js
- https://github.githubassets.com/assets/app_assets_modules_github_behaviors_commenting_edit_ts-app_assets_modules_github_behaviors_ht-83c235-c97eacdef68a.js
- https://github.githubassets.com/assets/app_assets_modules_github_blob-anchor_ts-app_assets_modules_github_filter-sort_ts-app_assets_-e5f169-c54621d9e188.js
- https://github.githubassets.com/assets/behaviors-3647463f0628.js
- https://github.githubassets.com/assets/vendors-node_modules_delegated-events_dist_index_js-node_modules_github_catalyst_lib_index_js-623425af41e1.js
- https://github.githubassets.com/assets/notifications-global-4dc6f295cc92.js
- https://github.githubassets.com/assets/vendors-node_modules_optimizely_optimizely-sdk_dist_optimizely_browser_es_min_js-node_modules-089adc-2328ba323205.js
- https://github.githubassets.com/assets/optimizely-1c55a525615e.js
- https://github.githubassets.com/assets/vendors-node_modules_virtualized-list_es_index_js-node_modules_github_template-parts_lib_index_js-c3e624db1d89.js
- https://github.githubassets.com/assets/vendors-node_modules_github_remote-form_dist_index_js-node_modules_delegated-events_dist_inde-911b971-b9c79ae563e3.js
- https://github.githubassets.com/assets/app_assets_modules_github_ref-selector_ts-8f8b76ecd8d3.js
- https://github.githubassets.com/assets/codespaces-700c7a36b916.js
- https://github.githubassets.com/assets/vendors-node_modules_github_mini-throttle_dist_decorators_js-node_modules_github_remote-form_-e3de2b-779fd9166293.js
- https://github.githubassets.com/assets/vendors-node_modules_github_file-attachment-element_dist_index_js-node_modules_github_filter--b2311f-15fe0f17a114.js
- https://github.githubassets.com/assets/repositories-0355d3fe50ee.js
- https://github.githubassets.com/assets/vendors-node_modules_github_remote-form_dist_index_js-node_modules_delegated-events_dist_index_js-0cc53ae22129.js
- https://github.githubassets.com/assets/topic-suggestions-b547ddd02b8c.js
- https://github.githubassets.com/assets/code-menu-da1cefc25b0a.js
- https://github.githubassets.com/assets/vendors-node_modules_github_remote-form_dist_index_js-node_modules_github_memoize_dist_esm_in-687f35-d131f0b6de8e.js
- https://github.githubassets.com/assets/sessions-2638decb9ee5.js

Certainty

Request

```
GET /MalshaImashi/Machine-learning-based-malware-detection HTTP/1.1
Host: github.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1244.7307 **Total Bytes Received** : 196804 **Body Length** : 193400 **Is Compressed** : No

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
ETag: W/"81e9554ee815e81ea2c816ffcef95e9c"
X-GitHub-Request-Id: CD12:0793:1011F26:11512CC:647A0639
Set-Cookie: _gh_sess=MzcJxePKrYiNzjL4nPNxXRKZVk4KvycnGkQaIldMsT%2BhiF403%2F16IrmG%2Bi1zH2G6HrIJnEFbmWMX
fLkY0mYRbKtdd6EIxnUP5rOTy%2B7fRP7cRm7vRifgw90mAMhrgRnstw3C3qeyu74WRgtGg%2FJtcbFc5CBMS4cltVnaFLhR1Lo4%2B
JJZa7lX4JGV5l1HFkxhcQogPcJr9IbAJL7VOmfxk%2FwS35JQUPXz9jm5XJKJz5KqUeRwDdUAbFmzLrE3OF5WoGYHlTUVZidhoReoYj
xa7w%3D%3D--CI38oZHfAAy5iGRj--kSd4OcXzede2olBI64b9dQ%3D%3D; Path=/; HttpOnly; Secure; SameSite=Lax
Set-Cookie: _octo=GH1.1.738414175.1685718585; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:0
9:45 GMT; Secure; SameSite=Lax
Set-Cookie: logged_in=no; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:09:45 GMT; HttpOnly; S
ecure; SameSite=Lax
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: GitHub.com
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Accept-Ranges: bytes
Referrer-Policy: no-referrer-when-downgrade
X-Frame-Options: deny
Vary: X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame, Accept-Encoding, Accept, X-Requested-With
Content-Type: text/html; charset=utf-8
Content-Security-Policy: default-src 'none'; base-uri 'self'; block-all-mixed-content; child-src githu
b.com/assets-cdn/worker/ gist.github.com/assets-cdn/worker/; connect-src 'self' uploads.github.com obje
cts-origin.githubusercontent.com www.githubstatus.com collector.github.com raw.githubusercontent.com ap
i.github.com github-cloud.s3.amazonaws.com github-production-repository-file-5c1aeb.s3.amazonaws.com gi
thub-production-upload-manifest-file-7fdce7.s3.amazonaws.com github-production-user-asset-6210df.s3.ama
zonaws.com cdn.optimizely.com logx.optimizely.com/v1/events *.actions.githubusercontent.com productionr
esultssa0.blob.core.windows.net/ productionresultssa1.blob.core.windows.net/ productionresultssa2.blob.
core.windows.net/ productionresultssa3.blob.core.windows.net/ productionresultssa4.blob.core.windows.ne
t/ wss://*.actions.githubusercontent.com github-production-repository-image-32fea6.s3.amazonaws.com git
hub-production-release-asset-2e65be.s3.amazonaws.com insights.github.com wss://alive.github.com; font-s
rc github.githubassets.com; form-action 'self' github.com gist.github.com objects-origin.githubusercont
ent.com; frame-ancestors 'none'; frame-src viewscreen.githubusercontent.com notebooks.githubuserconten
t.com; img-src 'self' data: github.githubassets.com media.githubusercontent.com camo.githubusercontent.
com identicons.github.com avatars.githubusercontent.com github-cloud.s3.amazonaws.com objects.githubuse
rcontent.com objects-origin.githubusercontent.com secured-user-images.githubusercontent.com/ user-image
s.githubusercontent.com/ private-user-images.githubusercontent.com opengraph.githubassets.com github-pr
oduction-user-asset-6210df.s3.amazonaws.com customer-stories-feed.github.com spotlights-feed.github.com
 *.githubusercontent.com; manifest-src 'self'; media-src github.com user-images.githubusercontent.com/
 secured-user-images.githubusercontent.com/ private-user-images.githubusercontent.com; script-src githu
b.githubassets.com; style-src 'unsafe-inline' github.githubassets.com; worker-src github.com/assets-cd
n/worker/ gist.github.com/assets-cdn/worker/
Date: Fri, 02
…
https://user-images.githubusercontent.com/">
<link rel="preconnect" href="https://github.githubassets.com" crossorigin>
```

```
<link rel="preconnect" href="https://avatars.githubusercontent.com">



<link crossorigin="anonymous" media="all" rel="stylesheet" href="https://github.githubassets.com/assets/light-0946cdc16f15.css" /><link crossorigin="anonymous" media="all" rel="stylesheet" href="https://github.githubassets.com/assets/dark-3946c959759a.css" /><link data-color-theme="dark_dimmed" crossorigin="anonymous" media="all" rel="stylesheet" data-href="https://github.githubassets.com/assets/dark_dimmed-9b9a8c91acc5.css" /><link data-color-theme="da
…
496cb79.css" /><link data-color-theme="dark_tritanopia" crossorigin="anonymous" media="all" rel="stylesheet" data-href="https://github.githubassets.com/assets/dark_tritanopia-aad6b801a158.css" />
<link crossorigin="anonymous" media="all" rel="stylesheet" href="https://github.githubassets.com/assets/primer-primitives-fb1d51d1ef66.css" />
<link crossorigin="anonymous" media="all" rel="stylesheet" href="https://github.githubassets.com/assets/primer-0e3420bbec16.css" />
<link crossorigin="anonymous" media="all" rel="stylesheet" href="https://github.githubassets.com/assets/global-0d04dfcdc794.css" />
<link crossorigin="anonymous" media="all" rel="stylesheet" href="https://github.githubassets.com/assets/github-c7a3a0ac71d4.css" />
<link crossorigin="anonymous" media="all" rel="stylesheet" href="https://github.githubassets.com/assets/code-9271f811184f.css" />

<meta name="optimizely-datafile" content="{&quot;groups&quot;: [], &quot;environmentKey&quot;: &quot;production&quot;, &quot;rollouts&quot;: [], &quot;typedAudiences&quot;: [], &quot;projectId
…
miss_protect_this_branch&quot;}, {&quot;experimentIds&quot;: [], &quot;id&quot;: &quot;21864370109&quot;, &quot;key&quot;: &quot;click.sign_in&quot;}], &quot;revision&quot;: &quot;1372&quot;}" />


<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/wp-runtime-14f3ad9684cf.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_stacktrace-parser_dist_stack-trace-parser_esm_js-node_modules_github_bro-a4c183-ae93d3fba59c.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/ui_packages_failbot_failbot_ts-e38c93eab86e.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/environment-de3997b81651.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_github_selector-observer_dist_index_esm_js-2646a2c533e3.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_github_relative-time-element_dist_index_js-99e288659d4f.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_fzy_js_index_js-node_modules_github_markdown-toolbar-element_dist_index_js-e3de700a4c9d.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_delegated-events_dist_index_js-node_modules_github_auto-complete-element-5b3870-ff38694180c6.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_github_file-attachment-element_dist_index_js-node_modules_github_
```

```
text-ex-3415a8-7ecc10fb88d0.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_github_filter-input-element_dist_index_js-node_modules_github_remote-inp-8873b7-5771678648e0.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_primer_view-components_app_components_primer_primer_js-node_modules_gith-3af896-d8cf3e5f5813.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/github-elements-6f05fe60d18a.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/element-registry-84be4ef284ec.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_lit-html_lit-html_js-9d9fe1859ce5.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_github_mini-throttle_dist_index_js-node_modules_github_alive-client_dist-bf5aa2-424aa982deef.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_github_turbo_dist_turbo_es2017-esm_js-ba0e4d5b3207.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_color-convert_index_js-node_modules_github_jtml_lib_index_js-40bf234a19dc.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_github_remote-form_dist_index_js-node_modules_scroll-anchoring_dist_scro-52dc4b-e1e33bfc0b7e.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_github_paste-markdown_dist_index_esm_js-node_modules_github_quote-select-743f1d-1b20d530fbf0.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/app_assets_modules_github_updatable-content_ts-dadb69f79923.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/app_assets_modules_github_behaviors_keyboard-shortcuts-helper_ts-app_assets_modules_github_be-f5afdb-3f05df4c282b.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/app_assets_modules_github_sticky-scroll-into-view_ts-050ad6637d58.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/app_assets_modules_github_behaviors_ajax-error_ts-app_assets_modules_github_behaviors_include-2e2258-7effad8d88d4.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/app_assets_modules_github_behaviors_commenting_edit_ts-app_assets_modules_github_behaviors_ht-83c235-c97eacdef68a.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/app_assets_modules_github_blob-anchor_ts-app_assets_modules_github_filter-sort_ts-app_assets_-e5f169-c54621d9e188.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/behaviors-3647463f0628.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_delegated-events_dist_index_js-node_modules_github_catalyst_lib_index_js-623425af41e1.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/notifications-global-4dc6f295cc92.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_optimizely_optimizely-sdk_dist_optimizely_browser_es_min_js-node_modules-089adc-2328ba323205.js"></script>
```

```
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/optimizely-1c55a525615e.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_virtualized-list_es_index_js-node_modules_github_template-parts_lib_index_js-c3e624db1d89.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_github_remote-form_dist_index_js-node_modules_delegated-events_dist_inde-911b971-b9c79ae563e3.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/app_assets_modules_github_ref-selector_ts-8f8b76ecd8d3.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/codespaces-700c7a36b916.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_github_mini-throttle_dist_decorators_js-node_modules_github_remote-form_-e3de2b-779fd9166293.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_github_file-attachment-element_dist_index_js-node_modules_github_filter--b2311f-15fe0f17a114.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/repositories-0355d3fe50ee.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_github_remote-form_dist_index_js-node_modules_delegated-events_dist_index_js-0cc53ae22129.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/topic-suggestions-b547ddd02b8c.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/code-menu-da1cefc25b0a.js"></script>


<title>GitHub - MalshaImashi/Machine-learning-based-malware-detection: Machine learning-based malware detection</title>



<meta name="route-pattern" content="/:user_id/:repository">




…
ull">
<span style="width: 0%;" data-view-component="true" class="Progress-item progress-pjax-loader-bar left-0 top-0 color-bg-accent-emphasis"></span>
</span>





<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/vendors-node_modules_github_remote-form_dist_index_js-node_modules_github_memoize_dist_esm_in-687f35-d131f0b6de8e.js"></script>
<script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/sessions-2638decb9ee5.js"></script>
```

```
<header class="Header-old header-logged-out js-details-container Details position-relative f4 py-3" rol
e="banner">
<button type="button" class="Header-backdrop d-lg-none border-0 position-fixed top
…
```

Remedy

Using Subresource Integrity is simply to add *integrity*attribute to the *script*tag along with a base64 encoded cryptographic hash value.

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js" integrity="sha384-
R4/ztc4ZlRqWjqIuvf6RX5yb/v90qNGx6fS48N0tRxiGkqveZETq72KgDVJCp2TC" crossorigin="anonymous"></script>
```

The hash algorithm must be one of **sha256**, **sha384**or **sha512**, followed by a '-' character.

External References

- Subresource Integrity
- Do not let your CDN betray you: Use Subresource Integrity
- Web Application Security with Subresource Integrity
- SRI Hash Generator

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

5. An Unsafe Content Security Policy (CSP) Directive in Use

INFORMATION ⓘ | 1

Netsparker detected that one of following CSP directives is used:

- unsafe-eval
- unsafe-inline

By using `unsafe-eval`, you allow the use of string evaluation functions like `eval`.

By using `unsafe-inline`, you allow the execution of inline scripts, which almost defeats the purpose of CSP. When this is allowed, it's very easy to successfully exploit a Cross-site Scripting vulnerability on your website.

Impact

An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully.

Vulnerabilities

5.1. https://github.com/MalshaImashi/Machine-learning-based-malware-detection

Unsafe Directive Used In Csp

- unsafe-inline

Certainty

Request

```
GET /MalshaImashi/Machine-learning-based-malware-detection HTTP/1.1
Host: github.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1244.7307 **Total Bytes Received :** 196804 **Body Length :** 193400 **Is Compressed :** No

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
ETag: W/"81e9554ee815e81ea2c816ffcef95e9c"
X-GitHub-Request-Id: CD12:0793:1011F26:11512CC:647A0639
Set-Cookie: _gh_sess=MzcJxePKrYiNzjL4nPNxXRKZVk4KvycnGkQaIldMsT%2BhiF403%2F16IrmG%2Bi1zH2G6HrIJnEFbmWMX
fLkY0mYRbKtdd6EIxnUP5rOTy%2B7fRP7cRm7vRifgw90mAMhrgRnstw3C3qeyu74WRgtGg%2FJtcbFc5CBMS4cltVnaFLhR1Lo4%2B
JJZa7lX4JGV5l1HFkxhcQogPcJr9IbAJL7VOmfxk%2FwS35JQUPXz9jm5XJKJz5KqUeRwDdUAbFmzLrE3OF5WoGYHlTUVZidhoReoYj
xa7w%3D%3D--CI38oZHfAAy5iGRj--kSd4OcXzede2olBI64b9dQ%3D%3D; Path=/; HttpOnly; Secure; SameSite=Lax
Set-Cookie: _octo=GH1.1.738414175.1685718585; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:0
9:45 GMT; Secure; SameSite=Lax
Set-Cookie: logged_in=no; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:09:45 GMT; HttpOnly; S
ecure; SameSite=Lax
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: GitHub.com
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Accept-Ranges: bytes
Referrer-Policy: no-referrer-when-downgrade
X-Frame-Options: deny
Vary: X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame, Accept-Encoding, Accept, X-Requested-With
Content-Type: text/html; charset=utf-8
Content-Security-Policy: default-src 'none'; base-uri 'self'; block-all-mixed-content; child-src githu
b.com/assets-cdn/worker/ gist.github.com/assets-cdn/worker/; connect-src 'self' uploads.github.com obje
cts-origin.githubusercontent.com www.githubstatus.com collector.github.com raw.githubusercontent.com ap
i.github.com github-cloud.s3.amazonaws.com github-production-repository-file-5c1aeb.s3.amazonaws.com gi
thub-production-upload-manifest-file-7fdce7.s3.amazonaws.com github-production-user-asset-6210df.s3.ama
zonaws.com cdn.optimizely.com logx.optimizely.com/v1/events *.actions.githubusercontent.com productionr
esultssa0.blob.core.windows.net/ productionresultssa1.blob.core.windows.net/ productionresultssa2.blob.
core.windows.net/ productionresultssa3.blob.core.windows.net/ productionresultssa4.blob.core.windows.ne
t/ wss://*.actions.githubusercontent.com github-production-repository-image-32fea6.s3.amazonaws.com git
hub-production-release-asset-2e65be.s3.amazonaws.com insights.github.com wss://alive.github.com; font-s
rc github.githubassets.com; form-action 'self' github.com gist.github.com objects-origin.githubusercont
ent.com; frame-ancestors 'none'; frame-src viewscreen.githubusercontent.com notebooks.githubuserconten
t.com; img-src 'self' data: github.githubassets.com media.githubusercontent.com camo.githubusercontent.
com identicons.github.com avatars.githubusercontent.com github-cloud.s3.amazonaws.com objects.githubuse
rcontent.com objects-origin.githubusercontent.com secured-user-images.githubusercontent.com/ user-image
s.githubusercontent.com/ private-user-images.githubusercontent.com opengraph.githubassets.com github-pr
oduction-user-asset-6210df.s3.amazonaws.com customer-stories-feed.github.com spotlights-feed.github.com
 *.githubusercontent.com; manifest-src 'self'; media-src github.com user-images.githubusercontent.com/
 secured-user-images.githubusercontent.com/ private-user-images.githubusercontent.com; script-src githu
b.githubassets.com; style-src 'unsafe-inline' github.githubassets.com; worker-src github.com/assets-cd
n/worker/ gist.github.com/assets-cdn/worker/
Date: Fri, 02
…
rc 'self'; media-src github.com user-images.githubusercontent.com/ secured-user-images.githubuserconten
t.com/ private-user-images.githubusercontent.com; script-src github.githubassets.com; style-src 'unsafe
```

```
-inline' github.githubassets.com; worker-src github.com/assets-cdn/worker/ gist.github.com/assets-cdn/w
orker/
Date: Fri, 02 Jun 2023 15:09:45 GMT
Content-Encoding:









<!DOCTYPE html>
<html lang="en
…
```

Remedy

If possible remove unsafe-evaland unsafe-inlinefrom your CSP directives.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP) HTTP Header
- Content Security Policy (CSP)

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

6. Cross-site Referrer Leakage through Referrer-Policy

INFORMATION ⓘ | 1   CONFIRMED | 1

Netsparker detected that `no-referrer-when-downgrade`is used in the Referrer-Policy declaration.

Impact

Referrer leakage is possible between two sites if they use either same or a higher protocol.

Vulnerabilities

6.1. https://github.com/MalshaImashi/Machine-learning-based-malware-detection

CONFIRMED

HttpHeaderRefererPolicy

- no-referrer-when-downgrade

Request

```
GET /MalshaImashi/Machine-learning-based-malware-detection HTTP/1.1
Host: github.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1244.7307 **Total Bytes Received :** 196804 **Body Length :** 193400 **Is Compressed :** No

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
ETag: W/"81e9554ee815e81ea2c816ffcef95e9c"
X-GitHub-Request-Id: CD12:0793:1011F26:11512CC:647A0639
Set-Cookie: _gh_sess=MzcJxePKrYiNzjL4nPNxXRKZVk4KvycnGkQaIldMsT%2BhiF403%2F16IrmG%2Bi1zH2G6HrIJnEFbmWMX
fLkY0mYRbKtdd6EIxnUP5rOTy%2B7fRP7cRm7vRifgw90mAMhrgRnstw3C3qeyu74WRgtGg%2FJtcbFc5CBMS4cltVnaFLhR1Lo4%2B
JJZa7lX4JGV5l1HFkxhcQogPcJr9IbAJL7VOmfxk%2FwS35JQUPXz9jm5XJKJz5KqUeRwDdUAbFmzLrE3OF5WoGYHlTUVZidhoReoYj
xa7w%3D%3D--CI38oZHfAAy5iGRj--kSd4OcXzede2olBI64b9dQ%3D%3D; Path=/; HttpOnly; Secure; SameSite=Lax
Set-Cookie: _octo=GH1.1.738414175.1685718585; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:0
9:45 GMT; Secure; SameSite=Lax
Set-Cookie: logged_in=no; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:09:45 GMT; HttpOnly; S
ecure; SameSite=Lax
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: GitHub.com
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Accept-Ranges: bytes
Referrer-Policy: no-referrer-when-downgrade
X-Frame-Options: deny
Vary: X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame, Accept-Encoding, Accept, X-Requested-With
Content-Type: text/html; charset=utf-8
Content-Security-Policy: default-src 'none'; base-uri 'self'; block-all-mixed-content; child-src githu
b.com/assets-cdn/worker/ gist.github.com/assets-cdn/worker/; connect-src 'self' uploads.github.com obje
cts-origin.githubusercontent.com www.githubstatus.com collector.github.com raw.githubusercontent.com ap
i.github.com github-cloud.s3.amazonaws.com github-production-repository-file-5c1aeb.s3.amazonaws.com gi
thub-production-upload-manifest-file-7fdce7.s3.amazonaws.com github-production-user-asset-6210df.s3.ama
zonaws.com cdn.optimizely.com logx.optimizely.com/v1/events *.actions.githubusercontent.com productionr
esultssa0.blob.core.windows.net/ productionresultssa1.blob.core.windows.net/ productionresultssa2.blob.
core.windows.net/ productionresultssa3.blob.core.windows.net/ productionresultssa4.blob.core.windows.ne
t/ wss://*.actions.githubusercontent.com github-production-repository-image-32fea6.s3.amazonaws.com git
hub-production-release-asset-2e65be.s3.amazonaws.com insights.github.com wss://alive.github.com; font-s
rc github.githubassets.com; form-action 'self' github.com gist.github.com objects-origin.githubusercont
ent.com; frame-ancestors 'none'; frame-src viewscreen.githubusercontent.com notebooks.githubuserconten
t.com; img-src 'self' data: github.githubassets.com media.githubusercontent.com camo.githubusercontent.
com identicons.github.com avatars.githubusercontent.com github-cloud.s3.amazonaws.com objects.githubuse
rcontent.com objects-origin.githubusercontent.com secured-user-images.githubusercontent.com/ user-image
s.githubusercontent.com/ private-user-images.githubusercontent.com opengraph.githubassets.com github-pr
oduction-user-asset-6210df.s3.amazonaws.com customer-stories-feed.github.com spotlights-feed.github.com
 *.githubusercontent.com; manifest-src 'self'; media-src github.com user-images.githubusercontent.com/
 secured-user-images.githubusercontent.com/ private-user-images.githubusercontent.com; script-src githu
b.githubassets.com; style-src 'unsafe-inline' github.githubassets.com; worker-src github.com/assets-cd
n/worker/ gist.github.com/assets-cdn/worker/
Date: Fri, 02
…
rt-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
```

```
Server: GitHub.com
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Accept-Ranges: bytes
Referrer-Policy: no-referrer-when-downgrade
X-Frame-Options: deny
Vary: X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame, Accept-Encoding, Accept, X-Requested-With
Content-Type: text/html; charset=utf-8
Content-Security-Policy: default-s
…
```

Remedy

See all available options and make sure that the current option really suits your need.

External References

- Referrer Policy
- Referrer-Policy - MDN
- A New Security Header: Referrer Policy
- Can I Use Referrer-Policy
- Referrer-Policy HTTP Header

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A6
SANS Top 25	200
OWASP Proactive Controls	C9
ISO27001	A.14.2.5

7. data: Used in a Content Security Policy (CSP) Directive

INFORMATION ⓘ | 1

Netsparker detected `data:`use in a CSP directive.

Impact

An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully by using `data:`protocol.

Vulnerabilities

7.1. https://github.com/MalshaImashi/Machine-learning-based-malware-detection

Data Directive Used

- data:

Certainty

Request

```
GET /MalshaImashi/Machine-learning-based-malware-detection HTTP/1.1
Host: github.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1244.7307 **Total Bytes Received :** 196804 **Body Length :** 193400 **Is Compressed :** No

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
ETag: W/"81e9554ee815e81ea2c816ffcef95e9c"
X-GitHub-Request-Id: CD12:0793:1011F26:11512CC:647A0639
Set-Cookie: _gh_sess=MzcJxePKrYiNzjL4nPNxXRKZVk4KvycnGkQaIldMsT%2BhiF403%2F16IrmG%2Bi1zH2G6HrIJnEFbmWMX
fLkY0mYRbKtdd6EIxnUP5rOTy%2B7fRP7cRm7vRifgw90mAMhrgRnstw3C3qeyu74WRgtGg%2FJtcbFc5CBMS4cltVnaFLhR1Lo4%2B
JJZa7lX4JGV5l1HFkxhcQogPcJr9IbAJL7VOmfxk%2FwS35JQUPXz9jm5XJKJz5KqUeRwDdUAbFmzLrE3OF5WoGYHlTUVZidhoReoYj
xa7w%3D%3D--CI38oZHfAAy5iGRj--kSd4OcXzede2olBI64b9dQ%3D%3D; Path=/; HttpOnly; Secure; SameSite=Lax
Set-Cookie: _octo=GH1.1.738414175.1685718585; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:0
9:45 GMT; Secure; SameSite=Lax
Set-Cookie: logged_in=no; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:09:45 GMT; HttpOnly; S
ecure; SameSite=Lax
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: GitHub.com
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Accept-Ranges: bytes
Referrer-Policy: no-referrer-when-downgrade
X-Frame-Options: deny
Vary: X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame, Accept-Encoding, Accept, X-Requested-With
Content-Type: text/html; charset=utf-8
Content-Security-Policy: default-src 'none'; base-uri 'self'; block-all-mixed-content; child-src githu
b.com/assets-cdn/worker/ gist.github.com/assets-cdn/worker/; connect-src 'self' uploads.github.com obje
cts-origin.githubusercontent.com www.githubstatus.com collector.github.com raw.githubusercontent.com ap
i.github.com github-cloud.s3.amazonaws.com github-production-repository-file-5c1aeb.s3.amazonaws.com gi
thub-production-upload-manifest-file-7fdce7.s3.amazonaws.com github-production-user-asset-6210df.s3.ama
zonaws.com cdn.optimizely.com logx.optimizely.com/v1/events *.actions.githubusercontent.com productionr
esultssa0.blob.core.windows.net/ productionresultssa1.blob.core.windows.net/ productionresultssa2.blob.
core.windows.net/ productionresultssa3.blob.core.windows.net/ productionresultssa4.blob.core.windows.ne
t/ wss://*.actions.githubusercontent.com github-production-repository-image-32fea6.s3.amazonaws.com git
hub-production-release-asset-2e65be.s3.amazonaws.com insights.github.com wss://alive.github.com; font-s
rc github.githubassets.com; form-action 'self' github.com gist.github.com objects-origin.githubusercont
ent.com; frame-ancestors 'none'; frame-src viewscreen.githubusercontent.com notebooks.githubuserconten
t.com; img-src 'self' data: github.githubassets.com media.githubusercontent.com camo.githubusercontent.
com identicons.github.com avatars.githubusercontent.com github-cloud.s3.amazonaws.com objects.githubuse
rcontent.com objects-origin.githubusercontent.com secured-user-images.githubusercontent.com/ user-image
s.githubusercontent.com/ private-user-images.githubusercontent.com opengraph.githubassets.com github-pr
oduction-user-asset-6210df.s3.amazonaws.com customer-stories-feed.github.com spotlights-feed.github.com
 *.githubusercontent.com; manifest-src 'self'; media-src github.com user-images.githubusercontent.com/
 secured-user-images.githubusercontent.com/ private-user-images.githubusercontent.com; script-src githu
b.githubassets.com; style-src 'unsafe-inline' github.githubassets.com; worker-src github.com/assets-cd
n/worker/ gist.github.com/assets-cdn/worker/
Date: Fri, 02
…
form-action 'self' github.com gist.github.com objects-origin.githubusercontent.com; frame-ancestors 'no
ne'; frame-src viewscreen.githubusercontent.com notebooks.githubusercontent.com; img-src 'self' data:gi
```

```
thub.githubassets.com media.githubusercontent.com camo.githubusercontent.com identicons.github.com avat
ars.githubusercontent.com github-cloud.s3.amazonaws.com objects.githubusercontent.com objects-
…
```

Remedy

Remove `data:`sources from your CSP directives.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP)
- Content Security Policy (CSP) HTTP Header

CLASSIFICATION

ISO27001	A.14.2.5

8. Disabled X-XSS-Protection Header

INFORMATION ⓘ | 1

Netsparker detected a disabled `X-XSS-Protection`header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

Internet Explorer's built-in cross-site scripting protection can be disabled by using the following HTTP Header : `X-XSS-Protection: 0`

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

8.1. https://github.com/MalshaImashi/Machine-learning-based-malware-detection

Header

- X-XSS-Protection: 0

Certainty

Request

```
GET /MalshaImashi/Machine-learning-based-malware-detection HTTP/1.1
Host: github.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1244.7307 **Total Bytes Received :** 196804 **Body Length :** 193400 **Is Compressed :** No

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
ETag: W/"81e9554ee815e81ea2c816ffcef95e9c"
X-GitHub-Request-Id: CD12:0793:1011F26:11512CC:647A0639
Set-Cookie: _gh_sess=MzcJxePKrYiNzjL4nPNxXRKZVk4KvycnGkQaIldMsT%2BhiF403%2F16IrmG%2Bi1zH2G6HrIJnEFbmWMX
fLkY0mYRbKtdd6EIxnUP5rOTy%2B7fRP7cRm7vRifgw90mAMhrgRnstw3C3qeyu74WRgtGg%2FJtcbFc5CBMS4cltVnaFLhR1Lo4%2B
JJZa7lX4JGV5l1HFkxhcQogPcJr9IbAJL7VOmfxk%2FwS35JQUPXz9jm5XJKJz5KqUeRwDdUAbFmzLrE3OF5WoGYHlTUVZidhoReoYj
xa7w%3D%3D--CI38oZHfAAy5iGRj--kSd4OcXzede2olBI64b9dQ%3D%3D; Path=/; HttpOnly; Secure; SameSite=Lax
Set-Cookie: _octo=GH1.1.738414175.1685718585; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:0
9:45 GMT; Secure; SameSite=Lax
Set-Cookie: logged_in=no; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:09:45 GMT; HttpOnly; S
ecure; SameSite=Lax
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: GitHub.com
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Accept-Ranges: bytes
Referrer-Policy: no-referrer-when-downgrade
X-Frame-Options: deny
Vary: X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame, Accept-Encoding, Accept, X-Requested-With
Content-Type: text/html; charset=utf-8
Content-Security-Policy: default-src 'none'; base-uri 'self'; block-all-mixed-content; child-src githu
b.com/assets-cdn/worker/ gist.github.com/assets-cdn/worker/; connect-src 'self' uploads.github.com obje
cts-origin.githubusercontent.com www.githubstatus.com collector.github.com raw.githubusercontent.com ap
i.github.com github-cloud.s3.amazonaws.com github-production-repository-file-5c1aeb.s3.amazonaws.com gi
thub-production-upload-manifest-file-7fdce7.s3.amazonaws.com github-production-user-asset-6210df.s3.ama
zonaws.com cdn.optimizely.com logx.optimizely.com/v1/events *.actions.githubusercontent.com productionr
esultssa0.blob.core.windows.net/ productionresultssa1.blob.core.windows.net/ productionresultssa2.blob.
core.windows.net/ productionresultssa3.blob.core.windows.net/ productionresultssa4.blob.core.windows.ne
t/ wss://*.actions.githubusercontent.com github-production-repository-image-32fea6.s3.amazonaws.com git
hub-production-release-asset-2e65be.s3.amazonaws.com insights.github.com wss://alive.github.com; font-s
rc github.githubassets.com; form-action 'self' github.com gist.github.com objects-origin.githubusercont
ent.com; frame-ancestors 'none'; frame-src viewscreen.githubusercontent.com notebooks.githubuserconten
t.com; img-src 'self' data: github.githubassets.com media.githubusercontent.com camo.githubusercontent.
com identicons.github.com avatars.githubusercontent.com github-cloud.s3.amazonaws.com objects.githubuse
rcontent.com objects-origin.githubusercontent.com secured-user-images.githubusercontent.com/ user-image
s.githubusercontent.com/ private-user-images.githubusercontent.com opengraph.githubassets.com github-pr
oduction-user-asset-6210df.s3.amazonaws.com customer-stories-feed.github.com spotlights-feed.github.com
 *.githubusercontent.com; manifest-src 'self'; media-src github.com user-images.githubusercontent.com/
 secured-user-images.githubusercontent.com/ private-user-images.githubusercontent.com; script-src githu
b.githubassets.com; style-src 'unsafe-inline' github.githubassets.com; worker-src github.com/assets-cd
n/worker/ gist.github.com/assets-cdn/worker/
Date: Fri, 02
…
15:09:45 GMT; HttpOnly; Secure; SameSite=Lax
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
```

```
Transfer-Encoding: chunked
Server: GitHub.com
X-Content-Type-Options: nosniff
X-XSS-Protection: 0

Accept-Ranges: bytes
Referrer-Policy: no-referrer-when-downgrade
X-Frame-Options: deny
Vary: X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame, Accept-Encoding, Accept, X-Requested-With
Content-
…
```

Remedy

Add the X-XSS-Protection header with a value of "1; mode= block".

-
  ```
  X-XSS-Protection: 1; mode=block
  ```

External References

- MSDN - Internet Explorer 8 Security Features
- X-XSS-Protection HTTP Header
- Internet Explorer 8 XSS Filter

CLASSIFICATION

SANS Top 25	693
WASC	15
OWASP Proactive Controls	C9
ISO27001	A.14.1.2

9. Missing object-src in CSP Declaration

INFORMATION ⓘ | 1

Netsparkerdetected that `object-src`is missed in CSP declaration. It allows the injection of plugins which can execute JavaScript.

Vulnerabilities

9.1. https://github.com/MalshaImashi/Machine-learning-based-malware-detection

Certainty

Request

```
GET /MalshaImashi/Machine-learning-based-malware-detection HTTP/1.1
Host: github.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1244.7307 **Total Bytes Received :** 196804 **Body Length :** 193400 **Is Compressed :** No

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
ETag: W/"81e9554ee815e81ea2c816ffcef95e9c"
X-GitHub-Request-Id: CD12:0793:1011F26:11512CC:647A0639
Set-Cookie: _gh_sess=MzcJxePKrYiNzjL4nPNxXRKZVk4KvycnGkQaIldMsT%2BhiF403%2F16IrmG%2Bi1zH2G6HrIJnEFbmWMX
fLkY0mYRbKtdd6EIxnUP5rOTy%2B7fRP7cRm7vRifgw90mAMhrgRnstw3C3qeyu74WRgtGg%2FJtcbFc5CBMS4cltVnaFLhR1Lo4%2B
JJZa7lX4JGV5l1HFkxhcQogPcJr9IbAJL7VOmfxk%2FwS35JQUPXz9jm5XJKJz5KqUeRwDdUAbFmzLrE3OF5WoGYHlTUVZidhoReoYj
xa7w%3D%3D--CI38oZHfAAy5iGRj--kSd4OcXzede2olBI64b9dQ%3D%3D; Path=/; HttpOnly; Secure; SameSite=Lax
Set-Cookie: _octo=GH1.1.738414175.1685718585; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:0
9:45 GMT; Secure; SameSite=Lax
Set-Cookie: logged_in=no; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:09:45 GMT; HttpOnly; S
ecure; SameSite=Lax
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: GitHub.com
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Accept-Ranges: bytes
Referrer-Policy: no-referrer-when-downgrade
X-Frame-Options: deny
Vary: X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame, Accept-Encoding, Accept, X-Requested-With
Content-Type: text/html; charset=utf-8
Content-Security-Policy: default-src 'none'; base-uri 'self'; block-all-mixed-content; child-src githu
b.com/assets-cdn/worker/ gist.github.com/assets-cdn/worker/; connect-src 'self' uploads.github.com obje
cts-origin.githubusercontent.com www.githubstatus.com collector.github.com raw.githubusercontent.com ap
i.github.com github-cloud.s3.amazonaws.com github-production-repository-file-5c1aeb.s3.amazonaws.com gi
thub-production-upload-manifest-file-7fdce7.s3.amazonaws.com github-production-user-asset-6210df.s3.ama
zonaws.com cdn.optimizely.com logx.optimizely.com/v1/events *.actions.githubusercontent.com productionr
esultssa0.blob.core.windows.net/ productionresultssa1.blob.core.windows.net/ productionresultssa2.blob.
core.windows.net/ productionresultssa
…
```

Remedy

Set `object-src`to `'none'`in CSP declaration:

```
Content-Security-Policy: object-src 'none';
```

CLASSIFICATION

SANS Top 25	16
WASC	15
OWASP Proactive Controls	C9
ISO27001	A.14.2.5

10. Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive

INFORMATION ⓘ | 1

Netsparker detected that wildcard was used in domain portion of a CSP directive.

Impact

This means you trust all of the subdomains of this domain, if this is the case there is no impact.

Vulnerabilities

10.1. https://github.com/MalshaImashi/Machine-learning-based-malware-detection

Wildcard Detected In Domain

- *.actions.githubusercontent.com

Certainty

Request

```
GET /MalshaImashi/Machine-learning-based-malware-detection HTTP/1.1
Host: github.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1244.7307 **Total Bytes Received** : 196804 **Body Length** : 193400 **Is Compressed** : No

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
ETag: W/"81e9554ee815e81ea2c816ffcef95e9c"
X-GitHub-Request-Id: CD12:0793:1011F26:11512CC:647A0639
Set-Cookie: _gh_sess=MzcJxePKrYiNzjL4nPNxXRKZVk4KvycnGkQaIldMsT%2BhiF403%2F16IrmG%2Bi1zH2G6HrIJnEFbmWMX
fLkY0mYRbKtdd6EIxnUP5rOTy%2B7fRP7cRm7vRifgw90mAMhrgRnstw3C3qeyu74WRgtGg%2FJtcbFc5CBMS4cltVnaFLhR1Lo4%2B
JJZa7lX4JGV5l1HFkxhcQogPcJr9IbAJL7VOmfxk%2FwS35JQUPXz9jm5XJKJz5KqUeRwDdUAbFmzLrE3OF5WoGYHlTUVZidhoReoYj
xa7w%3D%3D--CI38oZHfAAy5iGRj--kSd4OcXzede2olBI64b9dQ%3D%3D; Path=/; HttpOnly; Secure; SameSite=Lax
Set-Cookie: _octo=GH1.1.738414175.1685718585; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:0
9:45 GMT; Secure; SameSite=Lax
Set-Cookie: logged_in=no; Path=/; Domain=github.com; Expires=Sun, 02 Jun 2024 15:09:45 GMT; HttpOnly; S
ecure; SameSite=Lax
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: GitHub.com
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Accept-Ranges: bytes
Referrer-Policy: no-referrer-when-downgrade
X-Frame-Options: deny
Vary: X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame, Accept-Encoding, Accept, X-Requested-With
Content-Type: text/html; charset=utf-8
Content-Security-Policy: default-src 'none'; base-uri 'self'; block-all-mixed-content; child-src githu
b.com/assets-cdn/worker/ gist.github.com/assets-cdn/worker/; connect-src 'self' uploads.github.com obje
cts-origin.githubusercontent.com www.githubstatus.com collector.github.com raw.githubusercontent.com ap
i.github.com github-cloud.s3.amazonaws.com github-production-repository-file-5c1aeb.s3.amazonaws.com gi
thub-production-upload-manifest-file-7fdce7.s3.amazonaws.com github-production-user-asset-6210df.s3.ama
zonaws.com cdn.optimizely.com logx.optimizely.com/v1/events *.actions.githubusercontent.com productionr
esultssa0.blob.core.windows.net/ productionresultssa1.blob.core.windows.net/ productionresultssa2.blob.
core.windows.net/ productionresultssa3.blob.core.windows.net/ productionresultssa4.blob.core.windows.ne
t/ wss://*.actions.githubusercontent.com github-production-repository-image-32fea6.s3.amazonaws.com git
hub-production-release-asset-2e65be.s3.amazonaws.com insights.github.com wss://alive.github.com; font-s
rc github.githubassets.com; form-action 'self' github.com gist.github.com objects-origin.githubusercont
ent.com; frame-ancestors 'none'; frame-src viewscreen.githubusercontent.com notebooks.githubuserconten
t.com; img-src 'self' data: github.githubassets.com media.githubusercontent.com camo.githubusercontent.
com identicons.github.com avatars.githubusercontent.com github-cloud.s3.amazonaws.com objects.githubuse
rcontent.com objects-origin.githubusercontent.com secured-user-images.githubusercontent.com/ user-image
s.githubusercontent.com/ private-user-images.githubusercontent.com opengraph.githubassets.com github-pr
oduction-user-asset-6210df.s3.amazonaws.com customer-stories-feed.github.com spotlights-feed.github.com
 *.githubusercontent.com; manifest-src 'self'; media-src github.com user-images.githubusercontent.com/
 secured-user-images.githubusercontent.com/ private-user-images.githubusercontent.com; script-src githu
b.githubassets.com; style-src 'unsafe-inline' github.githubassets.com; worker-src github.com/assets-cd
n/worker/ gist.github.com/assets-cdn/worker/
Date: Fri, 02
…
itory-file-5c1aeb.s3.amazonaws.com github-production-upload-manifest-file-7fdce7.s3.amazonaws.com githu
b-production-user-asset-6210df.s3.amazonaws.com cdn.optimizely.com logx.optimizely.com/v1/events *.acti
```

```
ons.githubusercontent.comproductionresultssa0.blob.core.windows.net/ productionresultssa1.blob.core.win
dows.net/ productionresultssa2.blob.core.windows.net/ productionresultssa3.blob.core.windows.net/ produ
ctionresultssa4.blob.core.windows.net/ wss://*.actions.githubusercontent.comgithub-production-repositor
y-image-32fea6.s3.amazonaws.com github-production-release-asset-2e65be.s3.amazonaws.com insights.githu
b.com wss://alive.github.com; font-src github.githubassets.com; form-a
…
```

Remedy

If you trust all of the subdomains and if this is necessary then you do not need to take any actions. However if this is not the case replace the wildcard with the only subdomain that you trust.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP)
- Content Security Policy (CSP) HTTP Header

CLASSIFICATION

ISO27001	A.14.2.5

Show Scan Detail

Enabled Security Checks : Apache Struts S2-045 RCE,
Apache Struts S2-046 RCE,
BREACH Attack,
Code Evaluation,
Code Evaluation (Out of Band),
Command Injection,
Command Injection (Blind),
Content Security Policy,
Content-Type Sniffing,
Cookie,
Cross Frame Options Security,
Cross-Origin Resource Sharing (CORS),
Cross-Site Request Forgery,
Cross-site Scripting,
Cross-site Scripting (Blind),
Custom Script Checks (Active),
Custom Script Checks (Passive),

		Custom Script Checks (Per Directory), Custom Script Checks (Singular), Drupal Remote Code Execution, Expect Certificate Transparency (Expect-CT), Expression Language Injection, File Upload, Header Analyzer, Heartbleed, HSTS, HTML Content, HTTP Header Injection, HTTP Methods, HTTP Status, HTTP.sys (CVE-2015-1635), IFrame Security, Insecure JSONP Endpoint, Insecure Reflected Content, JavaScript Libraries, Local File Inclusion, Login Page Identifier, Mixed Content, Open Redirection, Referrer Policy, Reflected File Download, Remote File Inclusion, Remote File Inclusion (Out of Band), Reverse Proxy Detection, RoR Code Execution, Server-Side Request Forgery (DNS), Server-Side Request Forgery (Pattern Based), Server-Side Template Injection, Signatures, SQL Injection (Blind), SQL Injection (Boolean), SQL Injection (Error Based), SQL Injection (Out of Band), SSL, Static Resources (All Paths), Static Resources (Only Root Path), Unicode Transformation (Best-Fit Mapping), WAF Identifier, Web App Fingerprint, Web Cache Deception, WebDAV, Windows Short Filename, XML External Entity, XML External Entity (Out of Band)
URL Rewrite Mode	:	Heuristic
Detected URL Rewrite Rule(s)	:	None

<table>
<tr><td><b>Excluded URL Patterns</b></td><td>:</td><td>(log|sign)\-?(out|off)
exit
endsession
gtm\.js
WebResource\.axd
ScriptResource\.axd</td></tr>
<tr><td><b>Authentication</b></td><td>:</td><td>None</td></tr>
<tr><td><b>Scheduled</b></td><td>:</td><td>No</td></tr>
<tr><td><b>Additional Website(s)</b></td><td>:</td><td>None</td></tr>
</table>

This report created with 5.8.1.28119-master-bca4e4e
https://www.netsparker.com