

Forum:[Hack Forums](#)

Thread: [Working HTMLi/XSS on a \\$5B company. What next?](#)

Tjm - November 9, 2025, 4:19 pm

I'm not a professional, this is solely what I know and am working with, all of this was done manually with no automation, my knowledge is limited but I know there's smarter people here. My question is what could I try next.

I found a large, popular, wealth companies site where HTML/JS can be injected(Reflected only currently). This has been tested and allows for fake login panels with working keylogging(same page only), open redirect, Iframes aren't sandboxed, script tags aren't usable outside Iframe srcDoc(*Only tested this one use case* to check adding to localStorage in an attempt to work towards client sided persistence). Localstorage can be modified upon visit, same as the redirect obviously.

Js eval works if delivered inside HTML with the iframe inside and reaches the parent window location to redirect the entire page versus just the iframe, it wasn't necessary for the redirect as just HTML works but the eval function works. The website allows POST requests to be sent from the vulnerable page, not normal for the vector type(used it for test exfiltration of keylogged form data). LocalStorage can be modified but I couldn't do anything with gaining persistence because of same origin with service workers.

There are upload areas I haven't tested yet to see if I can somehow register a service worker for client side persistence. I'm thinking of testing to see if I can get autofill to drop the credentials so that it's a grab on visit or if the user clicked autofill not thinking. I can also call remote .js files from outside the domain for improved effectiveness in running code versus a long ass query string, which even if encoded still looks ehh to anyone with knowledge. Also stuff like remote download links can be added to the page to drop but of course it requires user interaction to run the file. CSP is missing object-src, default-src, script-src, and base-uri.

AGAIN I'M NO professional and learning more on the fly right now. Also the company does not give a flying f*** about this as I tried to notify(No PoC or hints at all so they can't ghost patch it) about the vulnerability.

Any ideas on what I should try next? I don't have intentions on using it it's more just learning. Within both white hat and black hat market what's this type of bounty worth? What are some ideas that could work to increase severity? Any outside the box ideas?

Thank you for reading this garbled mash of random info.

DramaKing - November 9, 2025, 4:36 pm

The company could "ghost patch" by combing logs and analyzing your requests. If the company is as large as you say, I would go to the media. That usually gets a fast response. An X post could do it, too.

Tjm - November 9, 2025, 4:58 pm

(Nov 9, 2025 05:36 PM)DramaKing Wrote: [CITE](#) The company could "ghost patch" by combing logs and analyzing your requests. If the company is as large as you say, I would go to the media. That usually gets a fast response. An X post could do it, too.

Yeah dude I don't understand why they aren't just responding to get the PoC. It's insane. It's been

working for over a month. I was using POST to exfil data but it's still a search bar. I thought about public disclosure. I highly doubt they're analyzing shit though lol, I've contacted every customer service, default security/admin emails, everything literally. No response hence why they aren't getting a remote hint to even what it is. Not looking for money more than just a professional large corporation to acknowledge something isn't right.

Edit:

I didn't consider media as much but just told them 90 days from my 5th contact attempt in every single contact method that exists that I'm going to publish an official report, never have done it but obviously not dumping the full exploit. I'll look into the correct way to do it without sounding shitty. Even though they are trash.

(Nov 9, 2025 05:36 PM)DramaKing Wrote: [\[CITE\]](#) The company could "ghost patch" by combing logs and analyzing your requests. If the company is as large as you say, I would go to the media. That usually gets a fast response. An X post could do it, too.

You think just wait 90 days and drop within reasonable boundaries on social to call them out? They are in fact huge, worth(vaguely) between \$4-5B USD, 2.3Mish followers on insta/FB. They sell products, licensed for specific type and the #1 in their market type.

0dayexploit - November 12, 2025, 4:39 am
can i see it?

Tjm - November 16, 2025, 2:10 am

(Nov 12, 2025 05:39 AM)0dayexploit Wrote: [\[CITE\]](#) can i see it?

There's 2 different sites now, just realized yesterday the other has the same vulns exactly, weird coincidence , completely different sites and companies same vulnerability as the \$4-5B guys. This one is more abled to be useful especially since it appeals to way more people.

I can't show any bit of it right now as much as I'd like to. Also just figured out if I place the login panel outside the Iframe instead, then on Iphone Safari if a user that's registered clicks the link it will prompt to autofill password, one click of that and FaceID(a lot of people use it) automatically submits the credentials too! ? So it takes only 2 clicks for an Iphone user to give up their login info; which could be for many sites.

Like

"Wow these are some kick ass "stuff they sell"

Clicks link, request for autofill, filled and submitted, then maybe redirect them back to a legitimate page on the site since it has an open redirect vulnerability chained to it.

Disclaimer I would never do this, this is all for general practice and theory

Edit: The user could either login/register in the same panel actually..