

Forum:[Hack Forums](#)

Thread: [Never Trust a Screenshot of Balance](#)

Deployed - November 8, 2019, 11:09 am

Hello HackForums, Deployed Here

Often a user dollar balance is requested before a transition of funds, and I want to emphasize that this is not efficient proof that he/she is actually a trustworthy or reputable member (or in this case, even has the balance at all). An inspect element tool is the most minimal form of manipulation when it comes to hacking, but can provide some misleading information upon request and be used for even worse alternatives.

I have posted a video in the Video Section to show you just how quickly it is (less than 5 seconds) to manipulate your Paypal balance for a screenshot (yes photoshop could work here too, but this is even easier than that). Essentially this is a tutorial video as well and therefore is posted in this section

How to prevent or be sure of balance?

Ask the user for a screen recording and require a refresh of the page in the minimal. This will undo any inspect element writing

Here is the video reference:

<https://hackforums.net/showthread.php?tid=6023277>

- Deployed

Zero - November 9, 2019, 3:16 am

This is so true. More people should be aware of this. Thank you

M0D3M - December 1, 2019, 9:31 pm

A page refresh is not sufficient proof either. Source override may be deployed with developer tools and still retain domain structure and SSL in URL box.

Wafflemonger - December 1, 2019, 9:58 pm

I'm honestly glad that someone bumped this thread. I've been meaning to ask a question, but didn't want to do it on anyone's sales thread where the gifs / short videos are shown.

People are so concerned about inspect element, and that's entirely true. But what's to stop someone from copying all the public HTML/CSS to their desktop and modifying it locally. Most of the time people never show the browser link, which means that there's no way to verify that the screen you're seeing is actually the site they claim.

For example: <https://i.imgur.com/vQ6oCG5.jpg>

If I refresh that page, it'll of course stay the same, because I modified the HTML. That literally took me 10 seconds to do the entire thing (including uploading to imgur). The only way you can be 100% sure of this is if the person shows the browser link AND refreshes by clicking the URL bar. This will ensure that the URL bar turns blue (highlighting your URL), then the person presses enter.

Makes sure no tricky post-processing is done.

ExpiredNumber - December 1, 2019, 10:36 pm

I definitely agree with the screen recording, ESPECIALLY. Because there's so many scams going on. Hopefully people will see this.

(Won't lie, it would be funny to joke to your friends, but honestly.. this is very helpful). Thank you for the YouTube. I'll spread it around.

Deployed - December 2, 2019, 8:44 am

(Dec 1, 2019 10:58 PM)Wafflemonger Wrote: [\[CITE\]](#) I'm honestly glad that someone bumped this thread. I've been meaning to ask a question, but didn't want to do it on anyone's sales thread where the gifs / short videos are shown.

People are so concerned about inspect element, and that's entirely true. But what's to stop someone from copying all the public HTML/CSS to their desktop and modifying it locally. Most of the time people never show the browser link, which means that there's no way to verify that the screen you're seeing is actually the site they claim.

For example: <https://i.imgur.com/vQ6oCG5.jpg>

If I refresh that page, it'll of course stay the same, because I modified the HTML. That literally took me 10 seconds to do the entire thing (including uploading to imgur). The only way you can be 100% sure of this is if the person shows the browser link AND refreshes by clicking the URL bar. This will ensure that the URL bar turns blue (highlighting your URL), then the person presses enter.

Makes sure no tricky post-processing is done.

Just like anything in life, a person can go to an exponential extent to commit fraud and essentially "get away with it". As you mentioned, even copying the source files will allow the user to refresh the page; so we request them to keep the url in the video. However, we also mentioned that source override is possible while keeping the original domain SSL visible; which therefore takes even more work! The moral is to be weary of users, especially if they are only showing you a simple screenshot. The more validations you require, the higher extent they will have to go to essentially lie to you.

Let's see how hard we can make them work. By evaluating their difficulty and original proof of funds we can gauge just how trustworthy they really are

- Deployed

Moon Clown - December 2, 2019, 8:49 am

True facts spoken here... So much can be changed it's hard to trust anyone in all reality.

Drowzy - December 9, 2019, 9:49 am

(Nov 8, 2019 12:09 PM)Deployed Wrote: [\[CITE\]](#) Hello HackForums, Deployed Here

Often a user dollar balance is requested before a transition of funds, and I want to emphasize that this is not efficient proof that he/she is actually a trustworthy or reputable member (or in this case, even has the balance at all). An inspect element tool is the most minimal form of manipulation when it comes to hacking, but can provide some misleading information upon request and be used for even worse alternatives.

I have posted a video in the Video Section to show you just how quickly it is (less than 5 seconds)

to manipulate your Paypal balance for a screenshot (yes photoshop could work here too, but this is even easier than that). Essentially this is a tutorial video as well and therefore is posted in this section

How to prevent or be sure of balance?

Ask the user for a screen recording and require a refresh of the page in the minimal. This will undo any inspect element writing

Here is the video reference:

<https://hackforums.net/showthread.php?tid=6023277>

- Deployed

I know about this but I just trust people till they give me a reason not to. Probably not a good thing to do