

Forum: [Hack Forums](#)

Thread: ['X-Frame Options Header not set' Question](#)

dapeamel - February 13, 2018, 8:34 am

Hello everyone,

now since two days ago I have tried to understand Clickjacking.

I think this article below describes it pretty well:

"Imagine an attacker who builds a web site that has a button on it that says "click here for a free iPod". However, on top of that web page, the attacker has loaded an iframe with your mail account, and lined up exactly the "delete all messages" button directly on top of the "free iPod" button. The victim tries to click on the "free iPod" button but instead actually clicked on the invisible "delete all messages" button. In essence, the attacker has "hijacked" the user's click, hence the name "Clickjacking".

source:

<https://www.lookingglasscyber.com/blog/threat-intelligence-insights/x-frame-options-clickjacking/>

I also read on Owasp about it.

I got a question though.

if the site is not protected against this attack.

I guess I have missed something... lack of knowledge but...

For instance if I am the "hacker", to be able to create that "invisible frame" that the user is clicking on from a mistake".

I need rights to write on the webpage? or how could I edit someone else webpage if I am not logged-on?

or do you edit the header in the request before you send it to the server for instance in Fiddler/Postman?

Please explain to me what I am misunderstood.

Thank you in advance

Baud - February 13, 2018, 10:44 am

I can make you two different examples, these should help you have a clearer understanding on how this attack works:

1) Generic case: you have access to a hacked website or a website you built yourself (the first option is obviously going to be more effective because a known website looks trusted, unlike a

sketchy domain your victim has never seen before), so you can edit the HTML code of each page to insert a little iframe tag and position it on top of the control that you want to hijack. It's as simple as that, but of course you need access to the control panel of the website or the ability to upload custom pages/files on the website.

2) LAN case: you have the ability to launch a MITM attack on a device connected to your same LAN, thus intercepting all the packets said device sends and receives, with the possibility to read and edit them at your own will. At this point since you have control over the traffic received by the targeted device, you can wait for the user to visit a specific website, and when it happens you intercept the request and inject the malicious frame code inside the HTML code of the web page which the browser of the victim will load once received. In this case you don't need access to the actual website but MITM attacks require you to be connected to the same local network as your target and more protected networks are immune to this kind of attack.

All this if X-Frame-Options are disabled of course.

dapeamel - February 13, 2018, 1:55 pm

(Feb 13, 2018 11:44 AM)Baud Wrote: [\[CITE\]](#) I can make you two different examples, these should help you have a clearer understanding on how this attack works:

1) Generic case: you have access to a hacked website or a website you built yourself (the first option is obviously going to be more effective because a known website looks trusted, unlike a sketchy domain your victim has never seen before), so you can edit the HTML code of each page to insert a little iframe tag and position it on top of the control that you want to hijack. It's as simple as that, but of course you need access to the control panel of the website or the ability to upload custom pages/files on the website.

2) LAN case: you have the ability to launch a MITM attack on a device connected to your same LAN, thus intercepting all the packets said device sends and receives, with the possibility to read and edit them at your own will. At this point since you have control over the traffic received by the targeted device, you can wait for the user to visit a specific website, and when it happens you intercept the request and inject the malicious frame code inside the HTML code of the web page which the browser of the victim will load once received. In this case you don't need access to the actual website but MITM attacks require you to be connected to the same local network as your target and more protected networks are immune to this kind of attack.

All this if X-Frame-Options are disabled of course.

Thank you a lot for a very clarified answer I found that very helpful I will look more into MITM attacks then.

I think I got a pretty good picture so far what I understood myself also the way you explained it.

when you say MITM attack on device connected to the same LAN.

If we play with the website I try to inject have disabled "X-Frame-Options", also I have created a user on the website.

Is it even then possible to do intercepting of all the packets cause I got limited access (as regular user) ?

The reason why I am asking cause, when i did the security scan I found 175 items that have 'X-Frame-Options Header Not Set'.

That's why I want to learn etc I have practised on DVWA and checked a bit on Owasps Wiki.

Thank you in advance.

Baud - *February 13, 2018, 2:01 pm*

You don't need an account on the website for the second method, you only need to be connected to the same LAN as your target. When launching a MITM attack you target a specific device and intercept all the packets it receives and sends, so all you have to do is intercept any random message containing a web page (you can do this very easily with zANTI for example, it's an Android app for MITM attacks), and edit the HTML code to insert your own malicious frame code. The code of course changes depending on what you want the frame to do when it's clicked, maybe you'd be interested in running some JavaScript code to get informations from the user, but this is up to you.