ABUSING TARGET

@s4n7h0

Statutory Warning

Disclaimer

“This presentation is purely intended for knowledge sharing. The presenter’s intention is not to show any unknown or zero day security bugs. I strongly encourage responsible disclosure if you encounter any similar issues in the wide internet range. Examples shown in the live demo is only for educational purpose.”

Target

- click here to foo

target	_blank _parent _self _top *framename*	Specifies where to open the linked document

Source: http://www.w3schools.com/tags/tag_a.asp

How it works (technically)

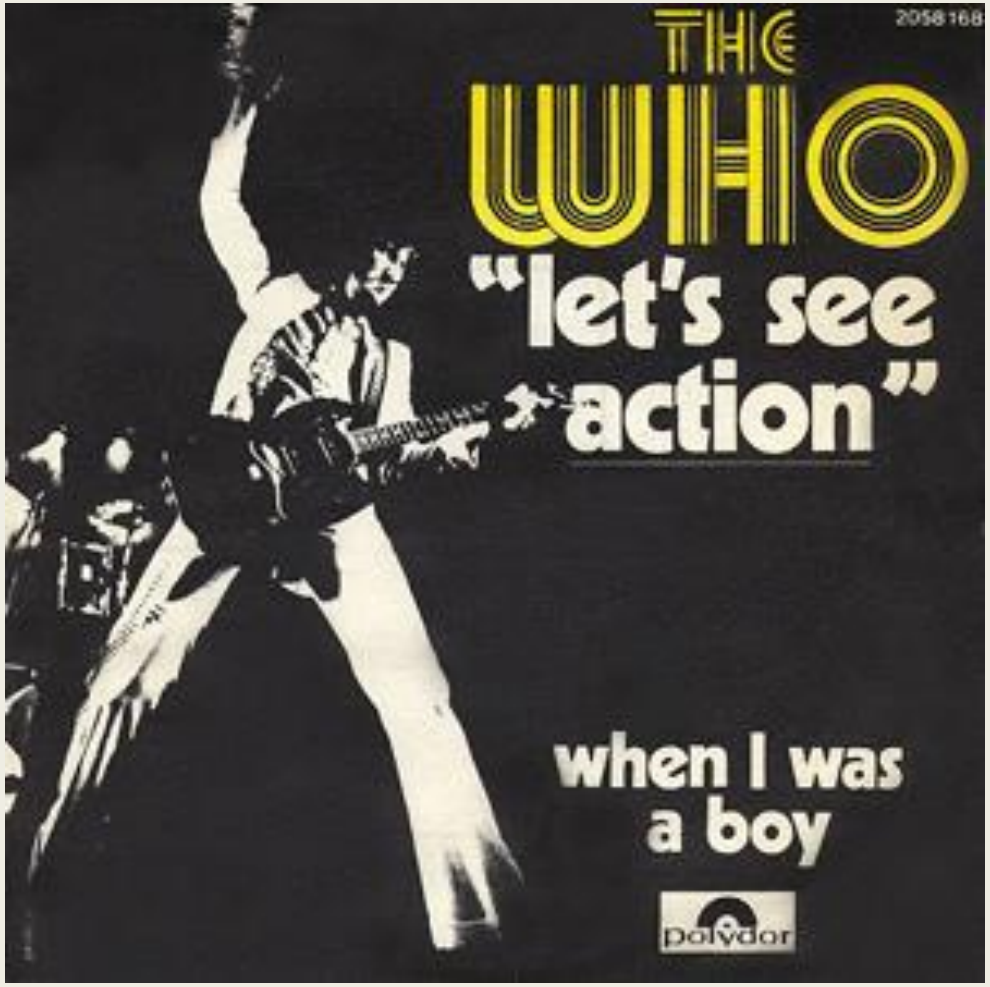
- User clicks on the hyperlink.
- The URL loads in new tab
- window.opener will have reference hook to parent tab.

window.opener

- Returns a reference to the window that opened this current window.
- Windows Phone browser does not support window.opener (tested with Microsoft Edge 25.10586.36.0). It is also not supported in IE if the opener is in a different security zone. (https://developer.mozilla.org/)

Source: http://www.w3schools.com/

Let’s see things in action



Alright, What’s the fix ?

- The issue is in client side, so does the fix too.
- Server can not control this.
- Security headers such as CSP, XXS Protection, etc., doesn't help.
- URL forwarding doesn't seems to have this issue so far.
- `rel="noopener noreferrer”`

Final thoughts

- Also known as _blank vulnerability. But somehow got ignored.
- There could be other sites that might have same issues. Go, hunt and report them responsibly.
- While some consider this as a security risk, others don't. Take your own mature decision on it.

Twitter: @s4n7h0

Email: i.am.s4n7h0@gmail.com