CLICKJACKING & PREVENTION TECHNIQUES

By Matt Langlois

WHOAMI

&

@

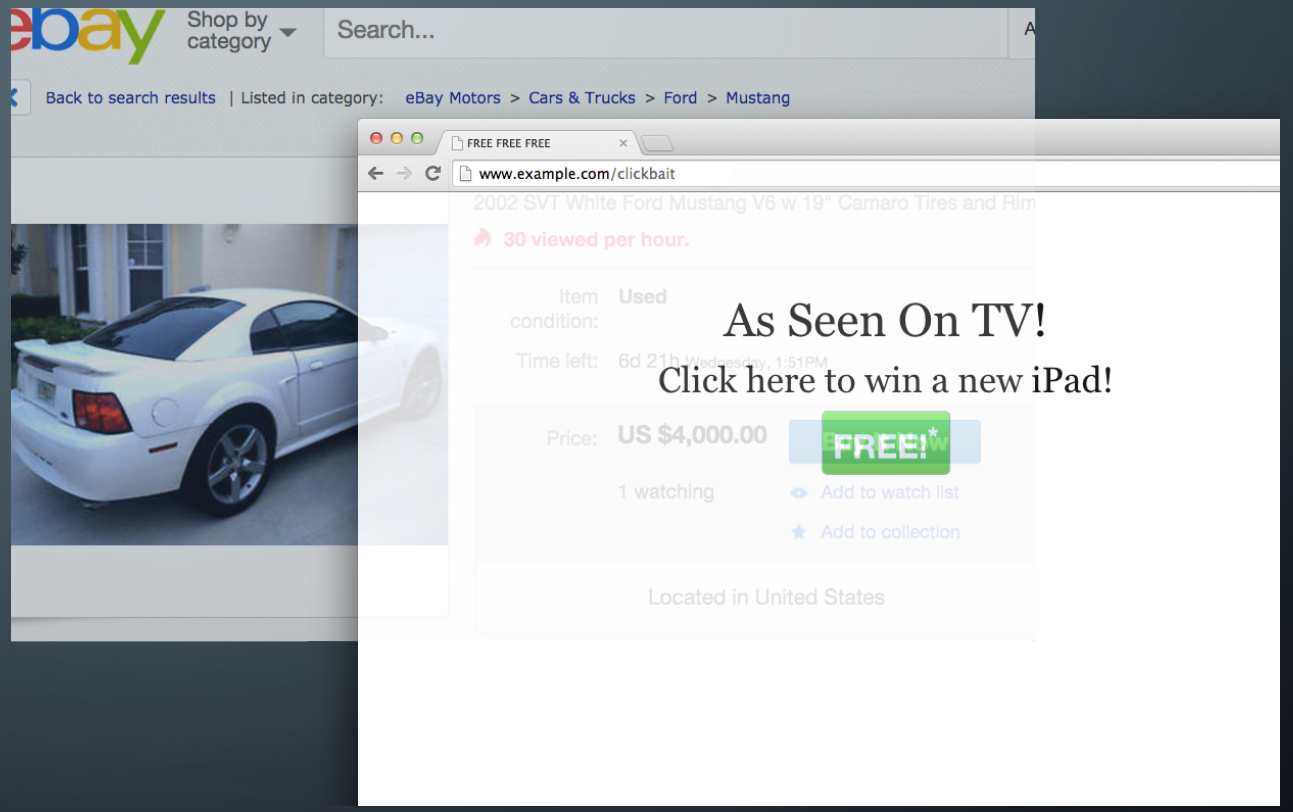
uOttawa

OUTLINE

- Clickjacking
  - Definition
  - Exploitation Techniques
- Preventing Clickjacking
  - Server side: The headers
  - Client Side: The framebusters
- Demonstration

CLICKJACKING: WHAT IS IT?

- A UI “redress”
- Tricking users into clicking something unintentionally
- Typically abuses websites which you have a session on



EXPLOITATION

- At its core to clickjack the user must be persuaded to click something they didn't intend to press
- Multiple types:
  - Likejacking (most common) – Abusing a user's session to gain likes/followers/retweets
  - Cursor jacking – Making the cursor appear a location, even though it is elsewhere
  - Password manager jacking – Tricking a password manager to reveal your password to the attacker (this actually happened with lastpass)

PREVENT YOUR SITE FROM BEING A TARGET

- The “X-Frame-Options” header to whitelist or deny framing
  - Prevents your website from being loaded into an iframe/frame
  - Supported in all major browsers for quite some time now (ie8 era)
  - Never “official” now deprecated in favor for CSP – however still reliable
- “Content-Security-Policy” header
  - Frame-ancestors option to whitelist specific URI’s which can load your site into a frame
  - The XFO header takes priority
- MUST BE AN HTTP RESPONSE HEADER, not a <meta> tag!
- But I need to develop for < IE8! Oh you poor soul…

LEGACY: FRAME BUSTING

- For those of who must develop for out of date browsers:

```
<style id="antiClickjack">body{display:none !important;}</style>
```

```
<script type="text/javascript">
   if (self === top) {
       var antiClickjack = document.getElementById("antiClickjack");
       antiClickjack.parentNode.removeChild(antiClickjack);
   } else {
       top.location = self.location;
   }
</script>
```

I CAN'T JUST PREVENT FRAMING, MY SITE IS FAMOUS!

- Window.confirm() is your friend

  OR

- Validate the user's action outside of the current window
- Don't rely on just JavaScript to perform framebusting!

I CAN HAZ UR LIKES

Demo of a facebook vulnerability I found while building this talk… The issue has been reported to facebook by me and I have permission to demo this

Please let me steal your facebook likes at (click demo link once page loads):

https://shorten.ninja/clickjacking

FACEBOOK'S RESPONSE

Our reply
Today
Hi Matt,

Facebook has a number plugin endpoints that were developed to be intentionally served within a frame on a third-party domain. For these endpoints, deploying X-Frame-Options or similar framebusting techniques is not a feasible option. The ability to perform a single action through these endpoints is not completely avoidable in low-volume testing. We mitigate the majority of these potential risks with backend heuristics to detect and remove suspicious actions occurring from these plugins. When possible, we trigger pop-up windows for final confirmation before performing certain actions. As a result, this style of clickjacking or "likejacking" vulnerability is not eligible under our bounty program. Sorry!

Thanks,

KEEP IN TOUCH!

- Github: https://github.com/fletchto99
- Twitter: @fletchto99
- Further reading: https://shorten.ninja/clickjacking
- Fun random website: https://pi.fletchto99.com
- Oh and that uOComputerSecurity page which you've already liked ☺