HTML5 Attacks

Pastejacking

ZDResearch
www.zdresearch.com

ZDResearch Advanced Web Hacking

Pastejacking

- Research about Paste Hijacking attack and create a legitimate web page which contains *apt-get install apache2* command
- Then in the above command embed the *nc -vvlp 8888 -e /bin/bash* command and when the victim runs *apt-get install apache2* the embedded command runs as well

Pastejacking - Solution

- You can find a basic Pastejacking exploit here:
  - https://github.com/dxa4481/Pastejacking/blob/master/index.html
- What this exploit actually do is change user clipboard when user is trying to copy the command
- How is that possible? It only takes the *keydown* event, then creates a hidden textarea and copies the content of the textarea (which contains the malicious command within)
  - User's browser copies the malicious command instead of the selected text
- This method only works when user tries to copy with the keyboard
- You can get the solution page from here:
  - https://exdemy.com/advanced-web-hacking/attachment/chapter05-pastejacking.html

ZDResearch Advanced Web Hacking
ZDResearch
www.zdresearch.com