FACEBOOK

OWASP Helsinki 2010-03-30

Markus Törnqvist
<mjt@fadconsulting.com>
FACEBOOK

Platform

- Canvas
- Iframe
- Connect
Languages

- FBML
- xFBML
- FBJS

PyFacebook for Python
FBjqRY for JavaScript
FBML and xFBML

- Not quite the same thing, some common
- fb:serverFbml – quite the kludge
- Good way to make things look like FB
- Bad how poorly customizable they are
FACEBOOK

FBJS

- Resembles normal JavaScript
- Disallowed words rewritten (alert and such)
- Supports ajax
- FBjqRY <3
Canvas

- Facebook acts as a proxy
- Content rewrite
- Interesting redirect bugs
Iframe

- No proxy, shown as-is
- Separate JavaScript handles xFBML
- Interesting redirect bugs again
FACEBOOK

Tabs

• Special case of Canvas
• Popular
• Changes UID :E
FACEBOOK

Tips

• Consider Facebook an insecure view
• Do not plan on storing data
• Use a secure library!
Tips

- CSRF tokens (as always)
- XSS can still happen
- Follow the news!