Clickjacking,
aneb tak trochu jiné klikáníčko

Roman Kümmel
ccuminn@soom.cz

Cross-Site Request Forgery (CSRF)

- Surfujete zatím po internetu zcela bezstarostně?
  - Možná by vám měla dělat starost zranitelnost CSRF, která
    - umožňuje zneužít vaší identitu přihlášeného uživatele
    - umožňuje zneužít vaší IP adresu
    - umožňuje napadnout zařízení ve vašem intranetu

- Aplikace by měli být ošetřeny autorizačním tokenem
  - u všech formulářů
  - u všech funkčních odkazů

Clickjacking

- Přichází na řadu ve chvíli, kdy jsou aplikace chráněny před CSRF
- Útočník může uživatele přimět k nevědomému vykonání akce
  - kliknutí na odkaz, tlačítko, nebo na jiný funkční prvek stránky
  - vyplnění a odeslání formuláře

- Dosáhnout toho lze
  - použitím průhledných rámů
  - překrytím nevhodných prvků
  - zneužitím funkčnosti Drag&Drop

Děkuji za pozornost