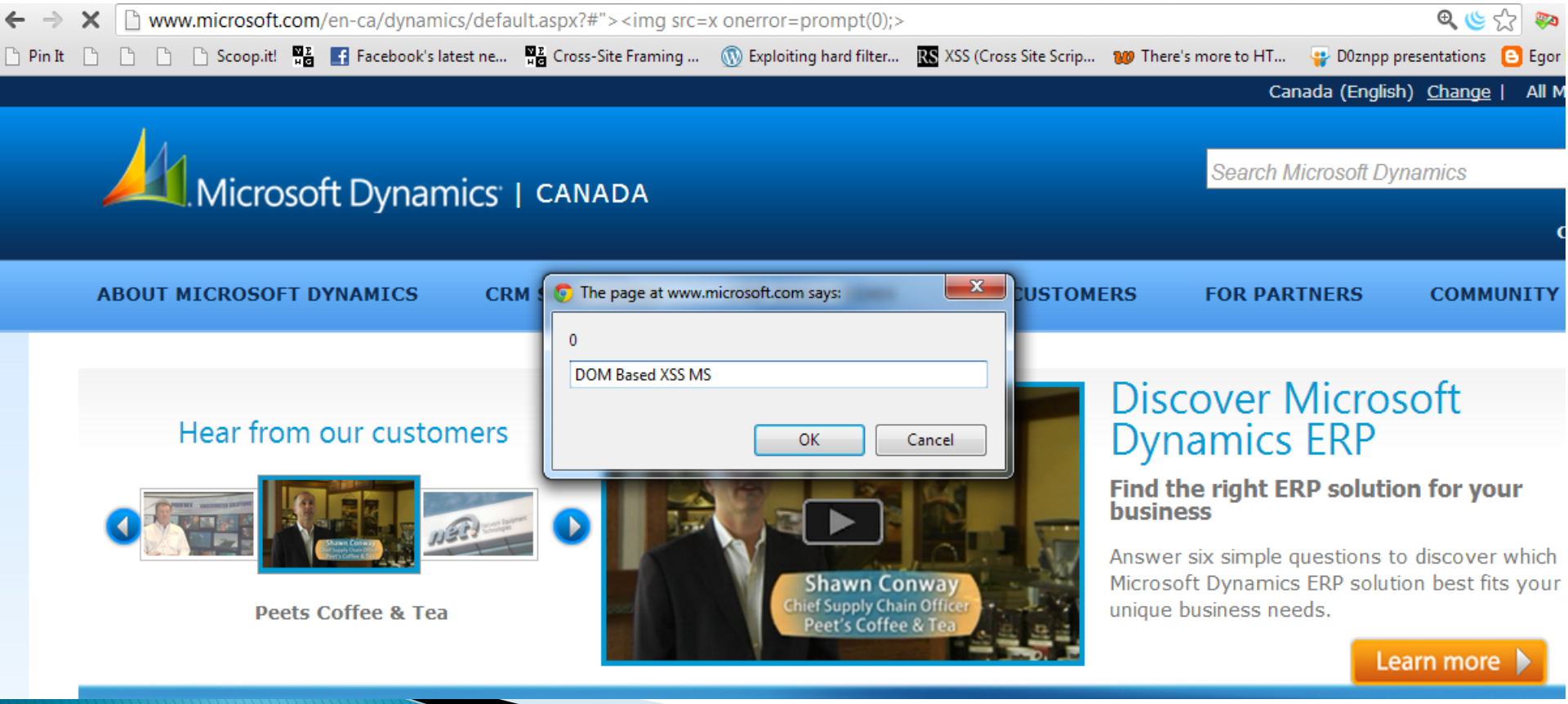
Technologie internetowe w programowaniu

Bezpieczeństwo aplikacji webowych

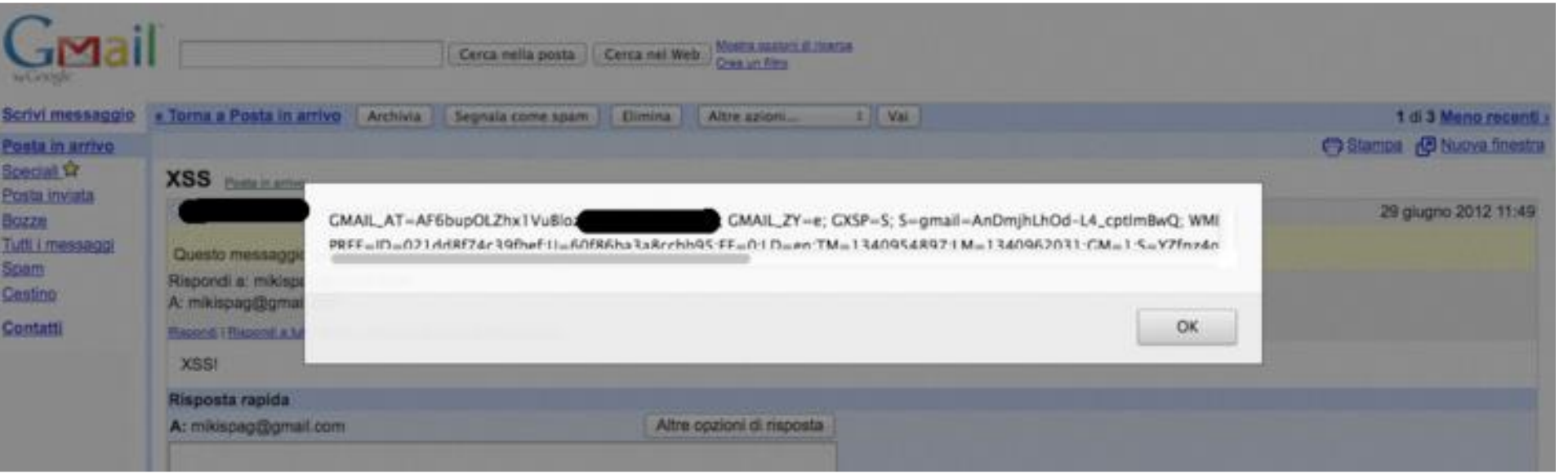
XSS

- Najczęściej występująca podatność

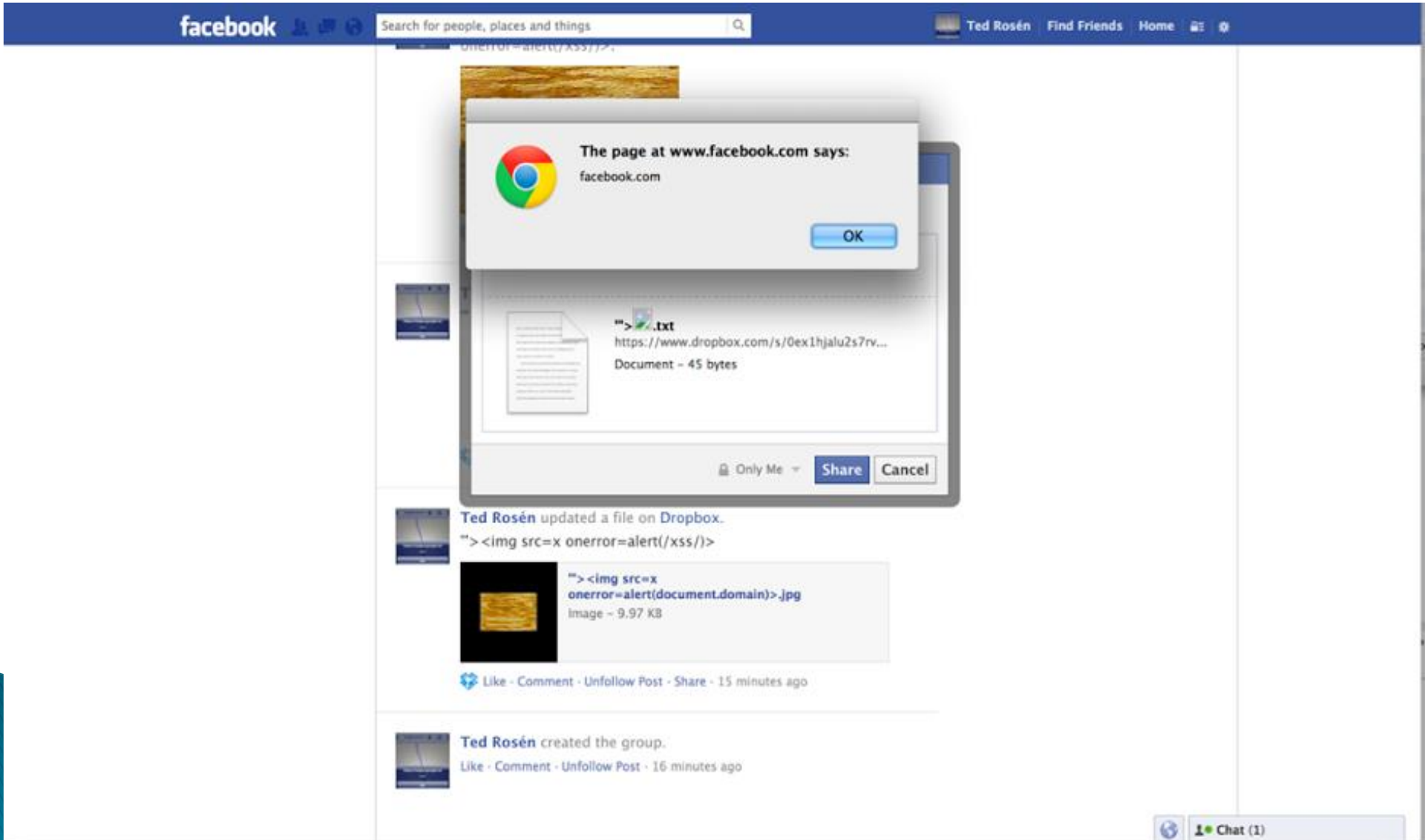


XSS

- Najczęściej występująca podatność



XSS


facebook
Search for people, places and things
Ted Rosén
Find Friends
Home
The page at www.facebook.com says:
facebook.com
OK
">.txt
https://www.dropbox.com/s/0ex1hjalu2s7rv...
Document - 45 bytes
Only Me
Share
Cancel
Ted Rosén updated a file on Dropbox.
"><img src=x onerror=alert(/xss/)>
"><img src=x onerror=alert(document.domain)>.jpg
Image - 9.97 KB
Like · Comment · Unfollow Post · Share · 15 minutes ago
Ted Rosén created the group.
Like · Comment · Unfollow Post · 16 minutes ago
Chat (1)

XSS

*andy
@derGeruhn

Blocked

<script class="xss">$('.xss').parents().eq(1).find('a').eq(1).click();$('[data-action=retweet]').click();alert('XSS in Tweetdeck')</script>❤

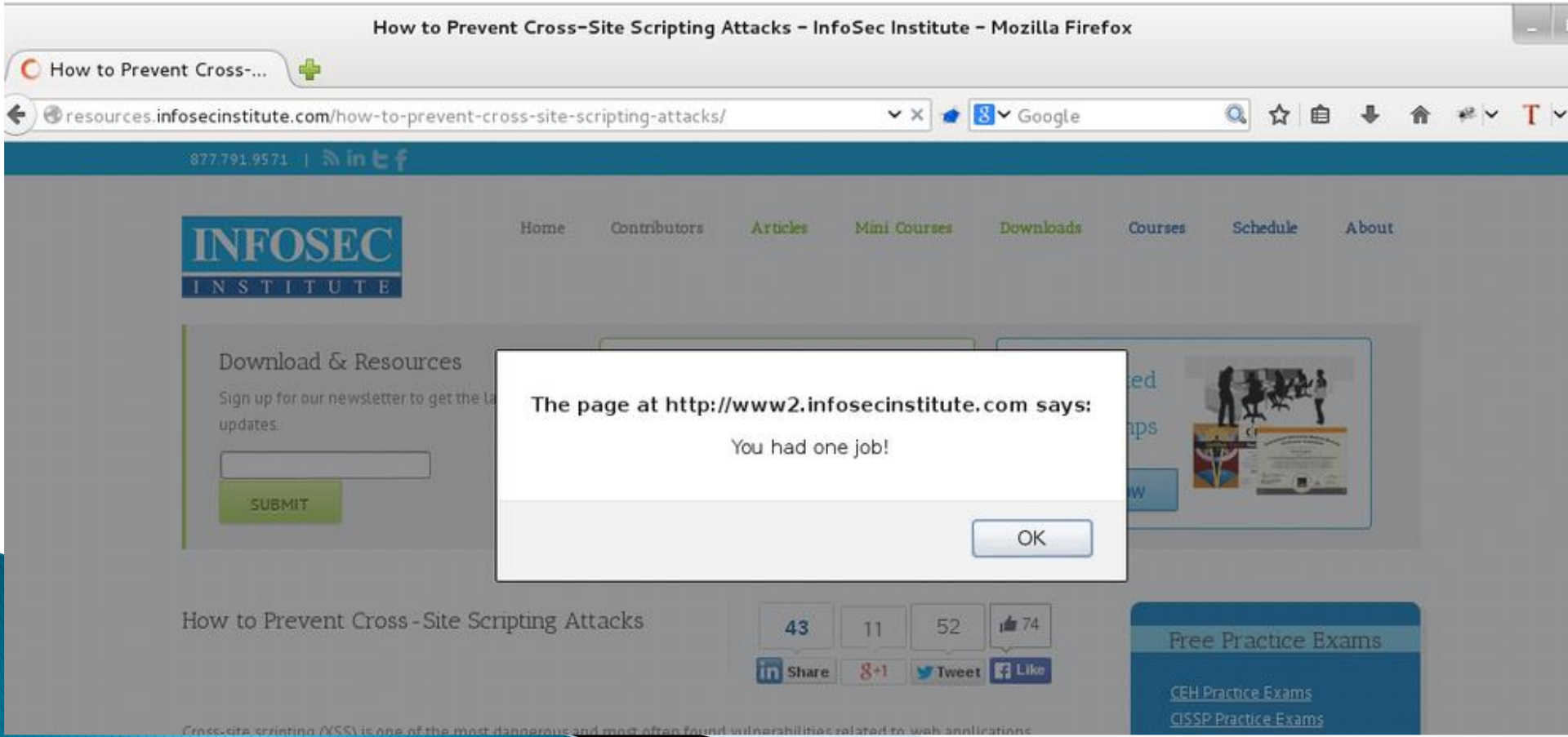
Reply Retweet Favorite ••• More

RETWEETS 39,027 FAVORITES 2,531

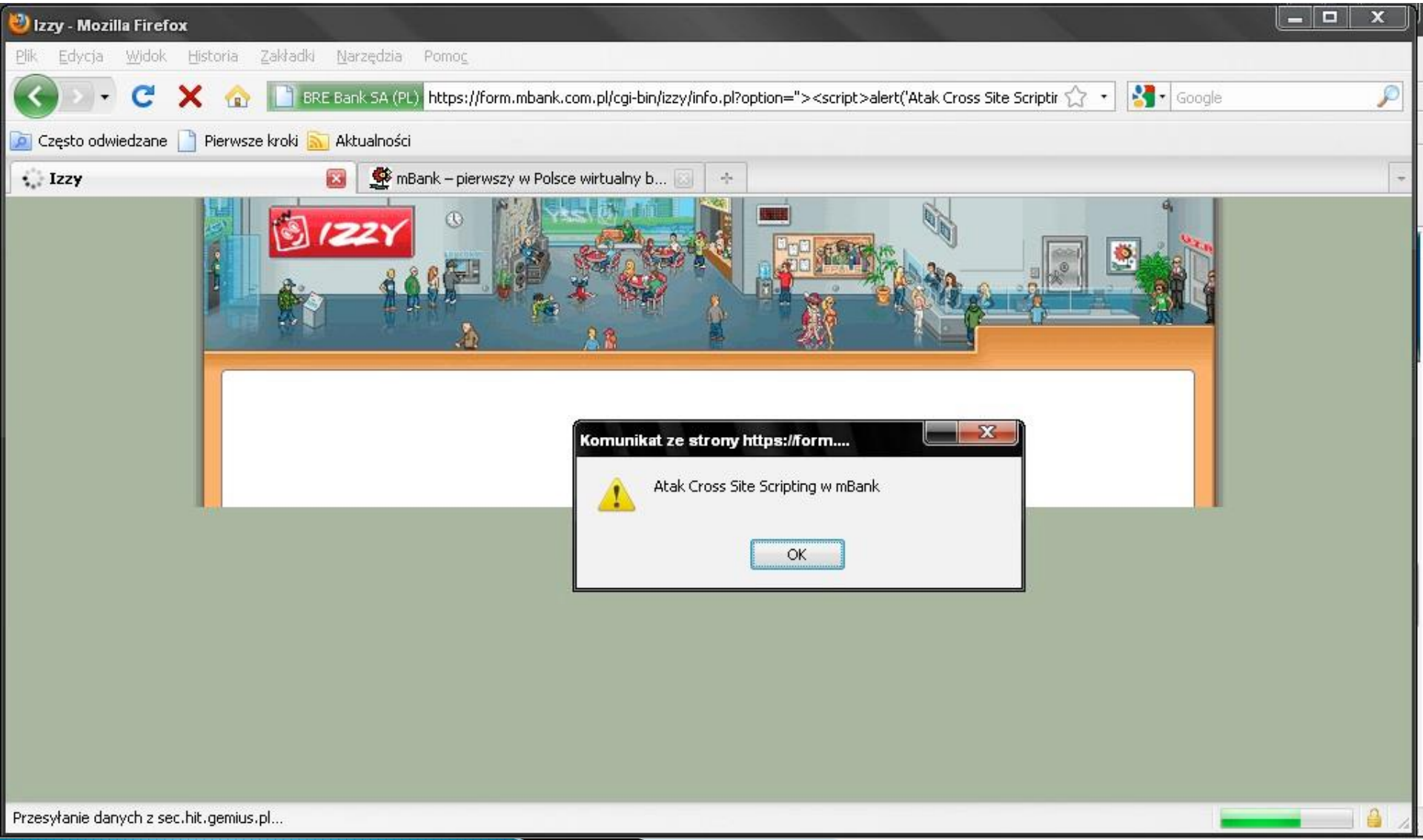
5:36 PM - 11 Jun 2014

XSS

- Najczęściej występująca podatność



XSS


Izzy - Mozilla Firefox
Plik Edycja Widok Historia Zakładki Narzędzia Pomoc
BRE Bank SA (PL)
https://form.mbank.com.pl/cgi-bin/izzy/info.pl?option="><script>alert('Atak Cross Site Scriptir
Google
Często odwiedzane
Pierwsze kroki
Aktualności
Izzy
mBank – pierwszy w Polsce wirtualny b...
IZZY
Komunikat ze strony https://form....
Atak Cross Site Scripting w mBank
OK
Przesyłanie danych z sec.hit.gemius.pl...

Skutki XSS

- **Kradzież danych** ze strony lub nagłówków HTTP, czyli…
  - Przejęcie konta użytkownika/admina
- **Deface:** przekierowanie użytkownika na inną stronę lub zasłonięcie obecnej
- **Skanowanie portów lokalnych**

Ćwiczenie

- Stwórz (korzystając z technologii *PHP* bądź HTML Web Strorage API) kod pozwalający na dodanie nowego tekstu (np. komentarza) na stronę internetową oraz podstronę wyświetlającą wszystkie dodane komentarze.
- Spróbuj wykonać atak typu XSS.
- Następnie spróbuj zabezpieczyć swoją stronę przed XSS za pomocą filtrowania wejścia.
- Sprawdź swoje zabezpieczenia korzystając z: https://gist.github.com/rvrsh3ll/09a8b933291f9f98e8ec#file-xxsfilterbypass-lst

Ochrona przed XSS

- Usunięcie przyczyny podatności
  - **Filtering** na wejściu
  - **Encoding** na wyjściu
- Wciąż wiele serwisów nie daje rady
  - Dlatego warto zaimplementować ochronę przed skutkami XSS.
- Content security policy
  - Pomysł Mozilla Fundation – pierwsza implementacja w Firefox 4.0
  - Ogólna idea: whitelista ładowanych zasobów

Content Security Policy

- Wsparcie w przeglądarkach:

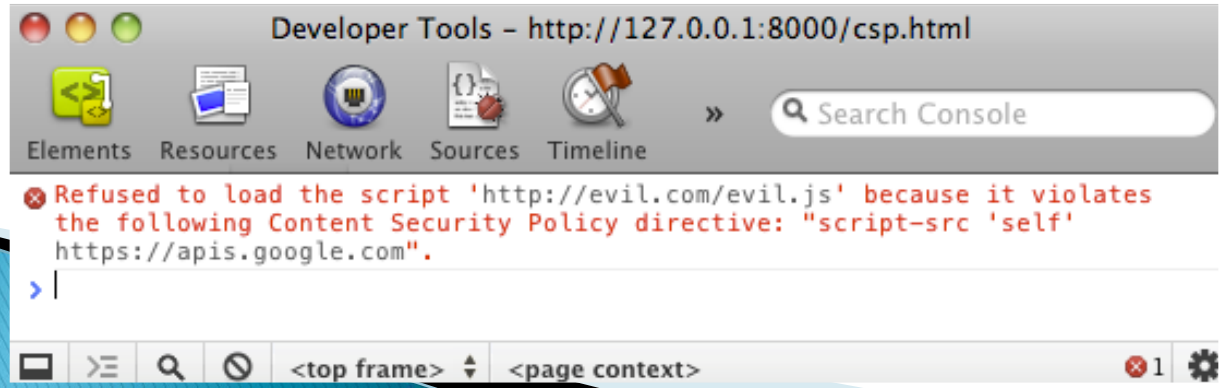
Content Security Policy 1.0 - CR

Mitigate cross-site scripting attacks by only allowing certain sources of script, style, and other resources.

Usage: Global — % of all users ? — 96.36% + 1.28% = 97.64%

Current aligned | Usage relative | Date relative | Filtered | All

IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Opera Mobile *	Chrome for Android	Firefox for Android	UC Browser for Android	Samsung Internet	QQ Browser	Bai Brow
				3.1-5		3.2-4.3									
		2-3.6	4-13	[2] 5.1		[2] 5.1									
6-9		[1] 4-22	[2] 14-24	[2] 6-6.1	10-12.1	[2] 6.1		2.1-4.3							
[1] 10	12-86	23-83	25-86	7-13.1	15-71	7-13.7		4.4-4.4.4	12-12.1				4-12.0		
[1] 11	87	84	87	14	72	14.3	all	81	59	87	83	[2] 12.12	13.0	10.4	7.1
		85-86	88-90	TP											



Content Security Policy

- Efekty uboczne:
  - brak obsługi skryptów inline **<script>trololo()</script>**
  - i eventów (np. **onerror, onclick**)
  - i urli **javascript:**
  - i tzw. “dynamic code evaluation” np. **eval()**
  - ani stylów inline’owych
- Poprawna implementacja przez:
  - zamianę na **addEventListener(…)**

Logowanie do aplikacji

- Popatrz na kod poniżej. Co należałoby przesłać do aplikacji aby zalogować się do niej (wykonanie bloku kodu dostępnego tylko dla zalogowanych osób) nie znając loginu i hasła?

```
$result = mysql_query("SELECT id FROM users where name='".
$login_box."' and pass='".$pass_box."'", $link);
$num_rows = mysql_num_rows($result);
if ($num_rows>0)
        {$stan=1;}

if ($stan==1)
        {echo('zalogowano');}
```

- Spróbuj to zamodelować i przetestować w swojej aplikacji.