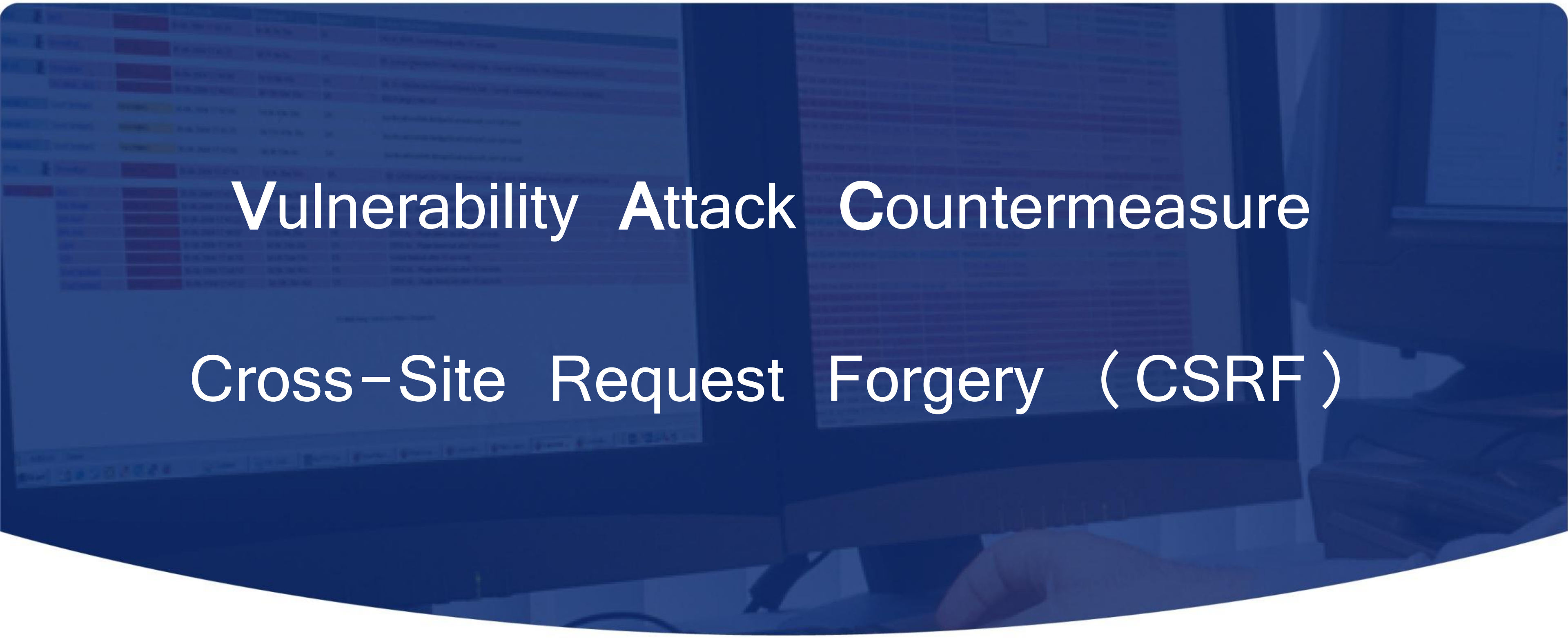
FOX-IT

EXPERTS IN IT SECURITY



Vulnerability Attack Countermeasure

Cross-Site Request Forgery （CSRF）

About me

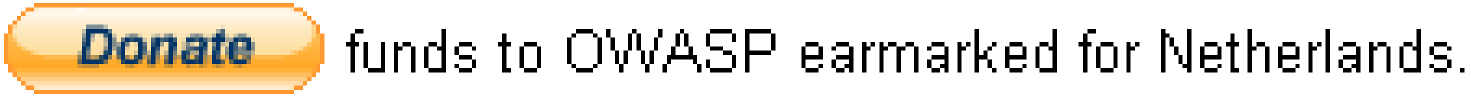
- Niels Teusink
- With Fox-IT since 2005
- IT Security Expert / Penetration Tester
- Personal blog: http://blog.teusink.net/

Vulnerability

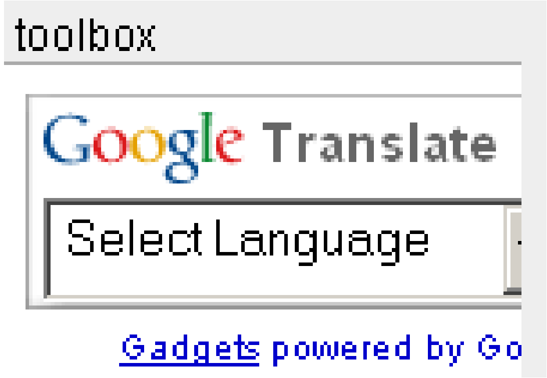
1. XSS
2. Injection flaws
3. Malicious file execution
4. Insecure direct object reference
5. CSRF
6. Information leakage & error handling
7. Broken authentication & sessions
8. Insecure crypto
9. Insecure communications
10. Failure to restrict URL access

OWASP Top 10 2007

Cross-Site?



Donate funds to OWASP earmarked for Netherlands.

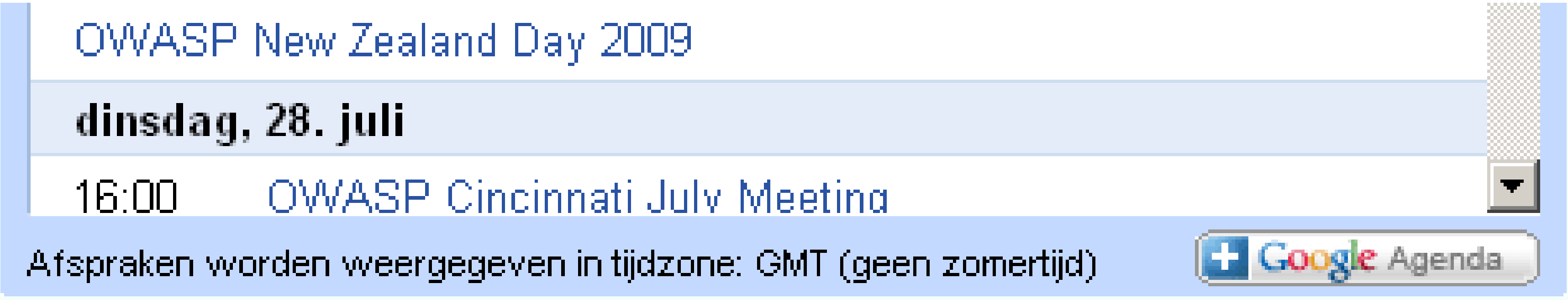


toolbox

Google Translate

Select Language

Gadgets powered by Go



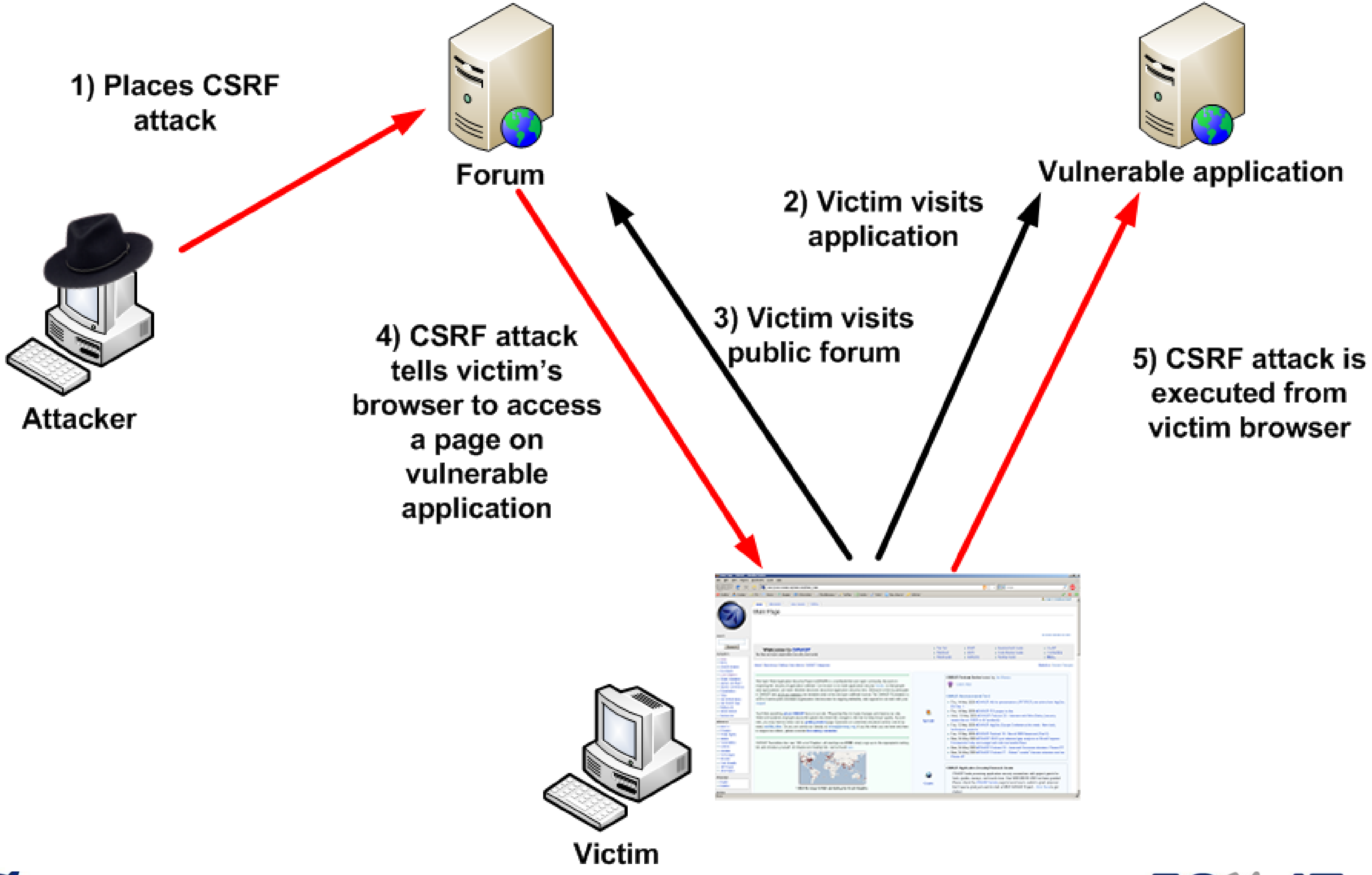
OWASP New Zealand Day 2009

dinsdag, 28. juli

16:00 OWASP Cincinnati July Meeting

Afspraken worden weergegeven in tijdzone: GMT (geen zomertijd)

How it works



1) Places CSRF attack

Forum

Vulnerable application

2) Victim visits application

3) Victim visits public forum

4) CSRF attack tells victim's browser to access a page on vulnerable application

5) CSRF attack is executed from victim browser

Attacker

Victim

Attack: A Case Study

December 2008: CSRF in Motorola ADSL2+ Modem

Attack: A Case Study (2)

```
<img src='http://192.168.1.254/
  Forms/remoteRES_1?NSS_RemotePas
  sword=ihackyou&NSS_EnableWANAdm
  inAccessRES=on&timeoutDisable=0
  &Enable=Enable'>
```

Attack: A Case Study (3)

- Now what?

- Steal provider credentials
- Modify DNS settings

Mantis Bug Tracker

```
http://www.example.com/mantis/manage_user_create.php?username=foo&realname=aa&password=aa&password_verify=aa&email=foo@attacker.com&access_level=90&protected=0&enabled=1
```

Effect: remote code execution

ING Direct

Felten & Zeller, 28-09-2008

1. Open a new account
2. Transfer money to new account
3. Add attacker as a contact
4. Transfer money to new contact

JSON Hijacking

Gmail, 01-01-2007

```
<script
  src='http://docs.google.com/dat
  a/contacts?out=js&show=ALL&psor
  t=Affinity&callback=google&max=
  99999'>
```

Countermeasure(s)

- Referrer checking
- CSRF token
- .NET ViewState
- Require extra information

Refer(r)er checking

- Where did you come from?
- Not a very good measure
  - Not everybody sends referrers
  - They can be spoofed
  - CSRF is not always ‘cross-site’

CSRF Token

- Every request contains a ‘secret’
  - Unique per session or request
- Example: OWASP CSRFGuard

CSRF Token

```
<form action='transfer.do' method='POST'>
Amount: <input name='amount'>
Account no: <input name='account'>
<input type='hidden' name='antiCSRF'
  value='23492408304834209'>
<input type='submit'>
</form>
```

.NET ViewState

- Only applicable to ASP.NET
- Using the ViewState to store a user-specific value
  - Don’t disable the MAC

Require extra information

- Password when changing password
- Password when changing profile
- CAPTCHA

But…

- Make sure you do not have any XSS vulnerabilities

Questions?

Resources

Interesting cases:

Motorola	http://www.neohaxor.org/2008/12/01/csrf-vulns-on-local-network-devices/
Simple Machines Forum	http://www.milw0rm.com/exploits/6993
DDWRT	http://archive.cert.uni-stuttgart.de/bugtraq/2008/12/msg00085.html
Mantis	http://www.ush.it/team/ush/hack-mantis111/adv.txt
ING Direct etc.	http://citp.princeton.edu/csrf/
Digg	http://4diggers.blogspot.com/

CSRF in general:

OWASP	http://www.owasp.org/index.php/Cross-Site_Request_Forgery
Wikipedia	http://en.wikipedia.org/wiki/Cross-site_request_forgery
Shiftlett.org	http://shiflett.org/articles/cross-site-request-forgeries

Books:

The Web Application Hacker’s Handbook – David Stuttard, Marcus Pinto

Contact

Fox−IT

Olof Palmestraat 6
P.O. Box 638
2600 AP Delft
The Netherlands
Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: fox@fox-it.com
Web www.fox-it.com

FOX-IT.COM