

Are your Domino Web Apps Secure?

Security Awareness Session by:
Ferdinand Vroom



BLUG
Belux Lotus User Group

Quick Show of Hands

Are you a...

- ☐ Developer?
- ☐ Administrator?
- ☐ User?
- ☐ Manager?
- ☐ Or all of The Above?



BLUG
Belux Lotus User Group

Agenda

- Latest & Worst Web App Vulnerabilities
- Some Vulnerabilities in the Wild
- OWASP
- Conclusions

Latest & Worst Web App Vulnerabilities

- Good Old XSS, Cross Site Scripting
- Drive- by Downloads
- CSRF, Cross Site Request Forgery
- XSHM, Cross- Site History Manipuation



BLUG
Belux Lotus User Group

XSS, Cross Site Scripting

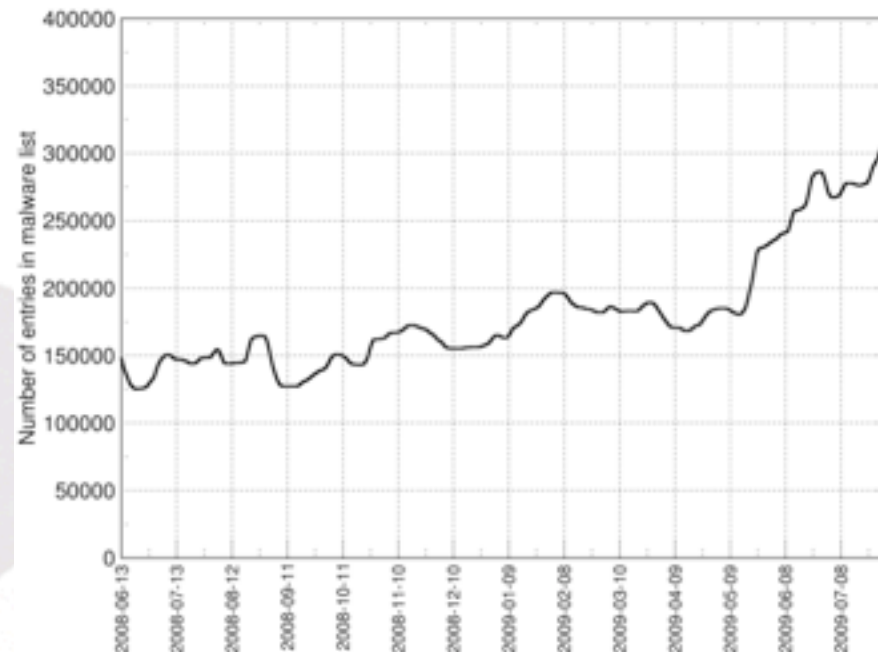
-  Stored
-  Reflected
-  Dom Based

XSS Cheat Sheet from RSnake:

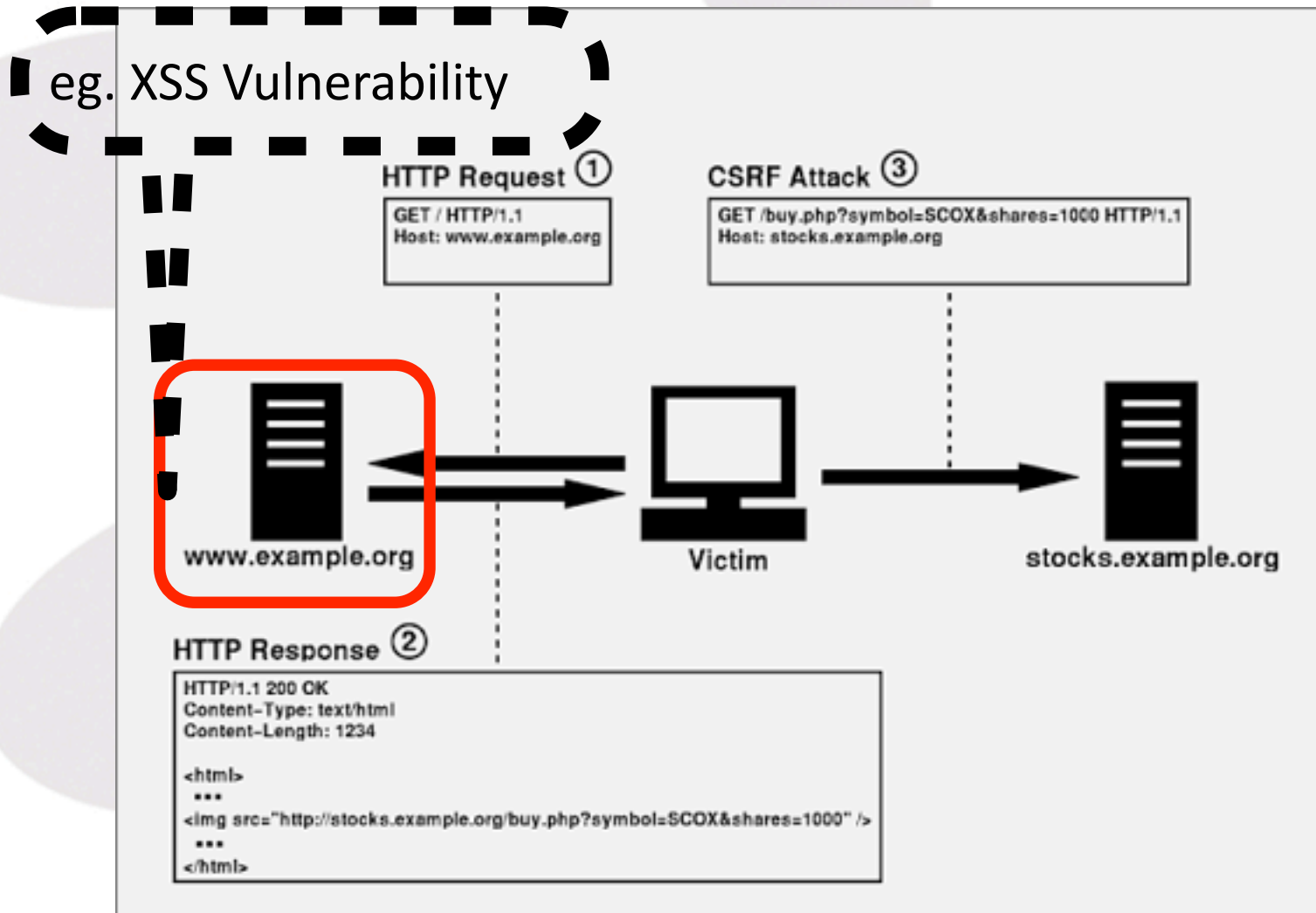
<http://ha.ckers.org/xss.html>

Drive- by Downloads

October 27, 2009: More than 640,000 Web sites and about 5.8 million pages are infected with malware.



CSRF, Cross Site Request Forgery



BLUG
Belux Lotus User Group

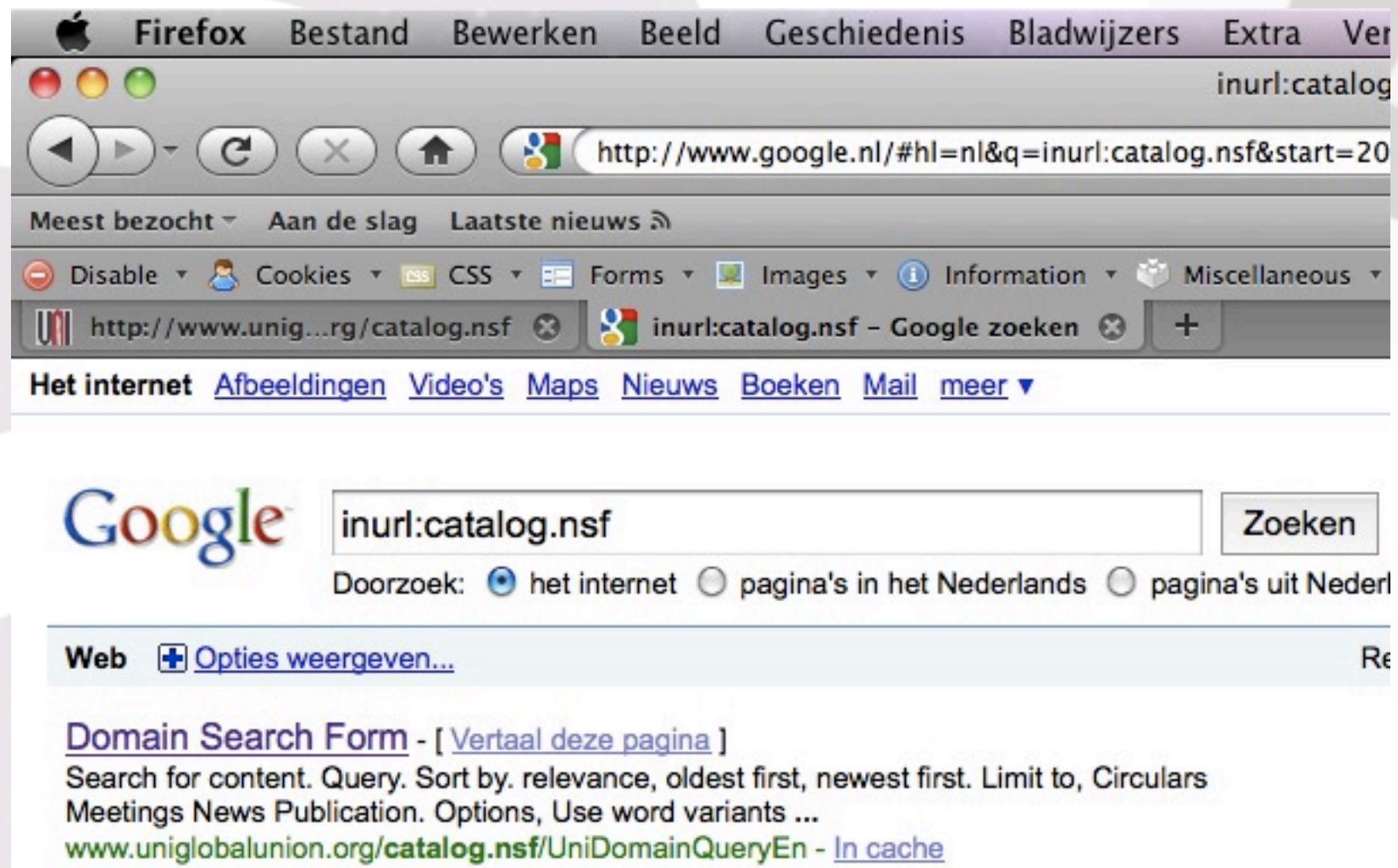
XSHM, Cross- Site History Manipulation

- Client Side Attack
- Trust Between User and Website
- SOP, Same Origin Policy, Breach
- Client Side Browser History



BLUG
Belux Lotus User Group

Mistakes by Admins, Devs, Management and Regulatory Bodies...



Firefox Bestand Bewerken Beeld Geschiedenis Bladwijzers Extra Venster Help
Mozilla Firefox

http://www.uniglobalunion.org/catalog.nsf

Meest bezocht - Aan de slag Laatste nieuws

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source

http://www.unig...rg/catalog.nsf inurkatalog.nsf - Google zoeken

Application Catalog

Search Help

Previous Page | Next Page | First Page | Last Page

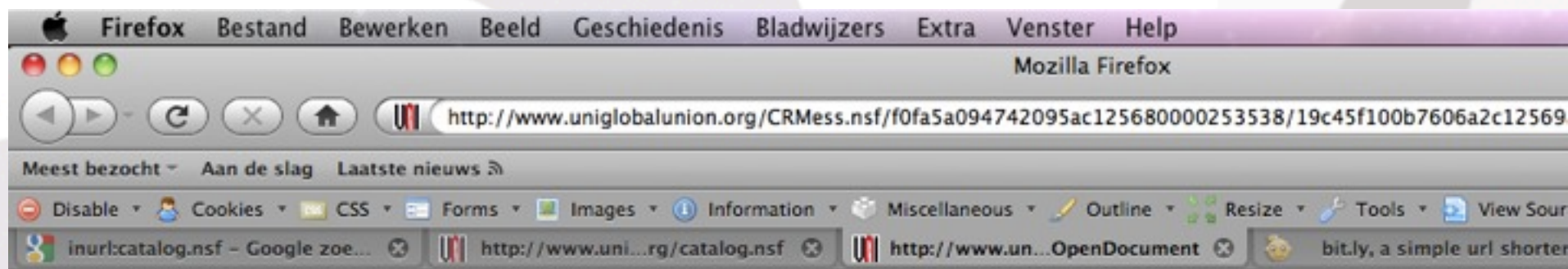
Domain Search

- Access Control Lists
 - By Application
 - By Level**
 - By Name
- Content
- Applications
- Domain Indexer Status
- File Systems

Access Level Title	Server	Access Control Lists\By Level File Name
1. Managers		
-Default-		
☐ BLOG UNI 2	Uniweb	BLOGUNiv100.NSF
☐ DECS Administrator	mail.union-network.org	decsadm.nsf
☐ DOLS Resource Template	mail.union-network.org	dolres.ntf
☐ DOLS Resource Template	Uni-Europa	dolres.ntf
☐ DOLS Resource Template	Uniweb	dolres.ntf
☐ Domino.Doc Admin Guide	Uni-Europa	ddmadmgd.nsf
☐ Domino.Doc User's Guide	Uni-Europa	ddmusrgd.nsf
☐ Lotus MTA Tables (v1.7)	mail.union-network.org	mtatbls.nsf
☐ Lotus MTA Tables (v1.7)	Uni-Europa	mtatbls.nsf
☐ Mail Jump	mail.union-network.org	mailjump.nsf
☐ Mail Jump	Uni-Europa	mailjump.nsf
☐ ScanMail Approve Database	mail.union-network.org	smdlsmdapproved.ntf
☐ SMTP MTA Tables (v4.7)	Uni-Europa	smtpbls.nsf
☐ Template Virtual Committee V 1.00	mail.union-network.org	TUNITVirtualCommitteesV100.ntf
☐ UNI Publications	mail.union-network.org	UNIPublications.nsf



BLUG
Belux Lotus User Group



Date: 23-11-2000
Category: doc

Title:
Several Documents

Text:



LN_Databases list.doc



Lotus_staff_groups.doc



Mobile phone numbers.doc



UNI Databases.doc



UNI Email address book groups.doc



UNI Sector and Group Abbreviations.doc



BLUG
Belux Lotus User Group



New registration - Step 1 of 2

Your username will be composed of your First Name + Middle Initial (if entered) + Last name.
(For example, Mary A Jones, Bob Smith or Chaka Khan)

Fields marked with an asterisk (*) are required

First Name*

Middle Initial:

Last Name*

[Continue](#)

[Start Over](#)



BLUG
Belux Lotus User Group

 New registration - Step 1 of 2

Your username will be composed of your First Name + Middle Initial (if entered) + Last name.
(For example, Mary A Jones, Bob Smith or Chaka Khan)

Fields marked with an asterisk (*) are required

First Name*

Middle Initial:

Last Name*

Continue

Start Over



BLUG
Belux Lotus User Group

Firefox

OpenNTE.org new user registration - Step 1

http://openntf.org/regerror.ns/n

Meest bezocht - Aan de slag - Laatste nieuws

BLUG: BLUG day event: March 3... Laden...

OpenNTE Registration - Error Message

We couldn't process your OpenNTE registration because the name you submitted,



De pagina op http://openntf.org meldt:
xss1

OK

Firefox

OpenNTE.org new user registration - Step 1

http://openntf.org/regerror.ns/n

Meest bezocht - Aan de slag - Laatste nieuws

BLUG: BLUG day event: March 3... Laden...

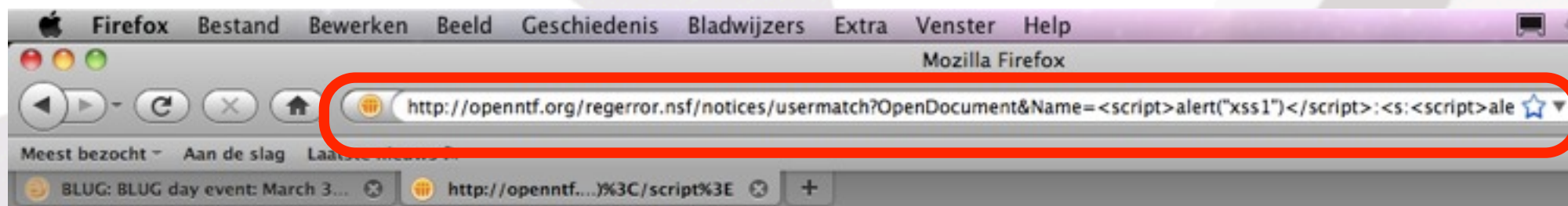
OpenNTE Registration - Error Message

We couldn't process your OpenNTE registration because the name you submitted,



De pagina op http://openntf.org meldt:
xss3

OK



OpenNTF Registration - Error Message

We couldn't process your OpenNTF registration because the name you submitted, ~~is already in use or not allowed.~~

[Please re-enter your username](#)

~~This time, try to enter a variation of your name. For example, if your name is Tom Smith, try Tom A. Smith or Thomas Smith.~~

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
```

```
<html>
```

```
<head>
```

```
<script language="JavaScript" type="text/javascript">
```

```
<!--
```

```
//Get query_string
```

```
var locstr = new String (location);
```

```
//find first name
```

```
var userindexfirst = locstr.indexOf("=");
```

```
var username = new String(locstr.substr(userindexfirst+1));
```

```
var userindexfirst = username.indexOf(":");
```

```
var firstusername = username.substr(0, userindexfirst);
```

```
//find middle Name
```

```
miduserstr = new String(username.substr(userindexfirst+1));
```

```
var userindexmid = miduserstr.indexOf(":");
```

```
var midusername = miduserstr.substr(0, userindexmid);
```

```
//find last Name
```

```
lastuserstr = new String(miduserstr.substr(userindexmid+1))
```

```
// -->
```

```
</script>
```

```
<script language="JavaScript" type="text/javascript">
```

```
<!--
```

```
document._domino_target = "_self";
```

```
function _doClick(v, o, t) {
```

```
    var returnValue = false;
```

```
    var url="/regerror.nsf/notices/usermatch?OpenDocument&Name=%3Cscript%3Ealert(%22xss1%22)
```

```
    if (o.href != null) {
```

```
        o.href = url;
```

```
        returnValue = true;
```

```
    } else {
```

```
        if (t == null)
```

```
            t = document._domino_target;
```

```
        window.open(url, t);
```

```
    }
```

```
    return returnValue;
```

```
}
```

```
// -->
```

```
</script>
```

```
</head>
```

```
<body text="#000000" bgcolor="#FFFFFF">
```

JavaScript Function for
Parsing the Query
String...

Our payload...



BLUG
Belux Lotus User Group

```

<body text="#000000" bgcolor="#FFFFFF">
<form action="">
<table border="0" cellspacing="0" cellpadding="0">
<tr valign="top"><td width="611"><b><font face="Arial">OpenNTF </font></b><b><font face="Arial">Registration - Error Message</font></b><br>
<br>
<font size="2" face="Arial">We couldn't process your OpenNTF registration because the name you</font><br>
<font size="2" face="Arial">submitted, </font> <FONT SIZE=2 FACE="Arial"><SCRIPT>document.write(unescape(firstusername)+" "+unescape(midusername)+" "+unescape(l
<br>
<a href="javascript:onclick=history.back()"><b><u><font size="2" color="#0000FF" face="Arial">Please re-enter your username</font></u></b></a><br>
<br>
<font size="2" face="Arial">This time, try to enter a variation of your name. For example, if your name is</font><br>
<font size="2" face="Arial">Tom Smith, try Tom A. Smith or Thomas Smith.</font></td></tr>
</table>
<div align="center"><br>
</div>
<input name="Error_Key" type="hidden" value="usermatch"></form>
</body>

```

<SCRIPT>document.write(unescape(firstusername)+" "+unescape(midusername))

Escaping/ Unescaping is
not Enough!



BLUG
Belux Lotus User Group



New registrati

```
<script>alert("123456789")</script>
```

```
<s
```

```
12345678901234567890123456789012345|
```

Your username will be composed of your First Name + Middle Initial (if entered) + Last name.
(For example, Mary A Jones, Bob Smith or Chaka Khan)

tekst

Fields marked with an asterisk (*) are required

First Name*

```
<script>alert("123456789")</script>
```

Middle Initial:

```
<s
```

Last Name*

```
12345678901234567890123456789012345|
```

Continue

Start Over

35 Characters, or...



BLUG
Belux Lotus User Group

```
<table cellpadding=4 border="0" cellspacing="0" cellpa
<tr valign="top"><td width="120"><font size="2" face="
<input name="FirstName" value="" SIZE=35 MAXLENGTH=35>

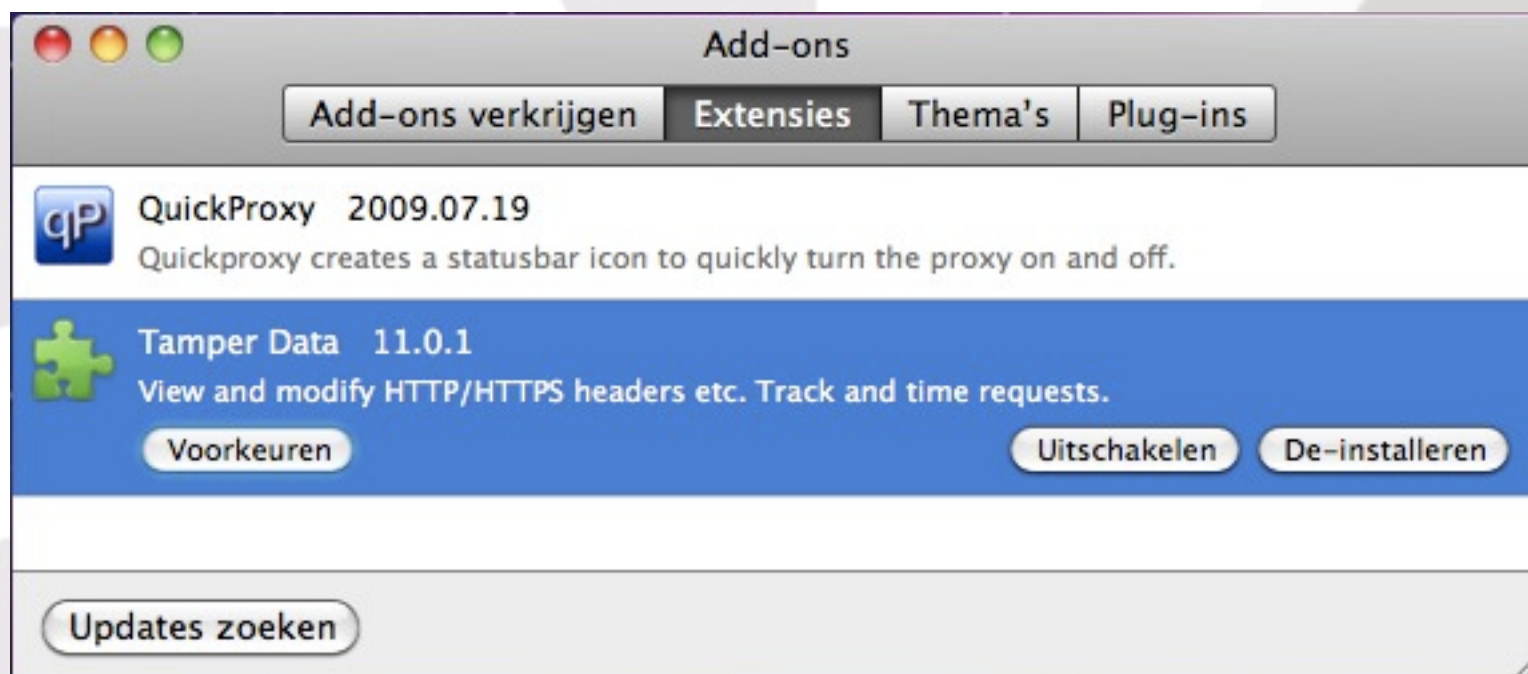
<tr valign="top"><td width="120"><font size="2" face="
<input name="MiddleInitial" value="" SIZE=2 MAXLENGTH=

<tr valign="top"><td width="120"><font size="2" face="
<input name="LastName" value="" SIZE=35 MAXLENGTH=35><
</table>
```

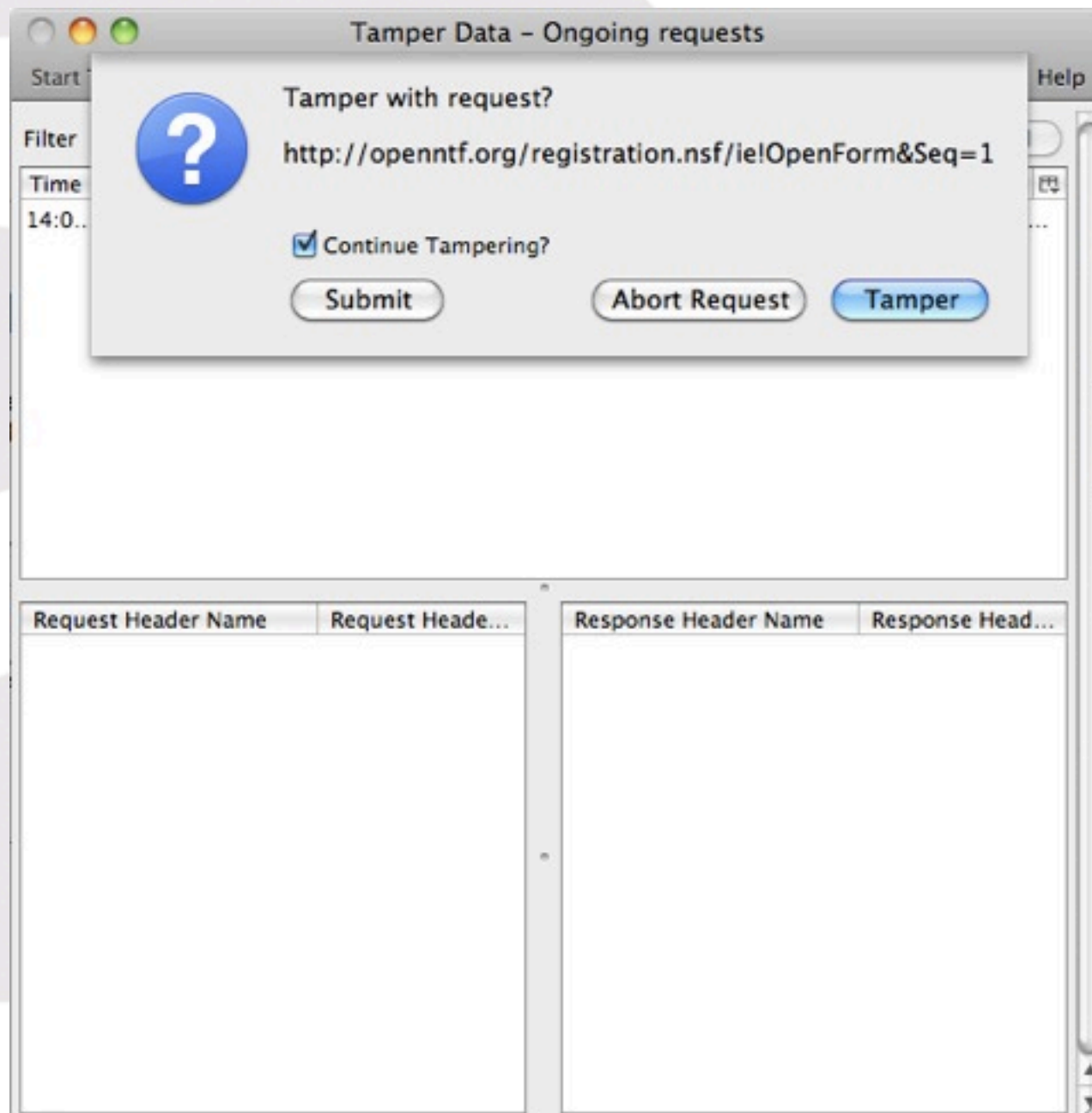
■ Clientside
■ inputvalidation...



BLUG
Belux Lotus User Group



BLUG
Belux Lotus User Group



BLUG
Belux Lotus User Group



Post Parameter Name	Post Parameter Value
__Click	0
FirstName	%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
MiddleInitial	%3Cs
LastName	12345678901234567890123456789012345

tekst

%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E



BLUG
Belux Lotus User Group



De pagina op <http://openntf.org> meldt:

__utma=51980151.487711806.1269808215.1269857426.1269861654.4;
__utmz=51980151.1269808215.1.1.utmccn=(direct)|utmcsr=
(direct)|utmcmd=(none); __utmb=51980151; __utmc=51980151;
SessionID=CI4KGZCTCR

OK



BLUG
Belux Lotus User Group

OWASP

-  Top Ten Risks
-  Guides
-  Tools
-  Models, Techniques & Frameworks



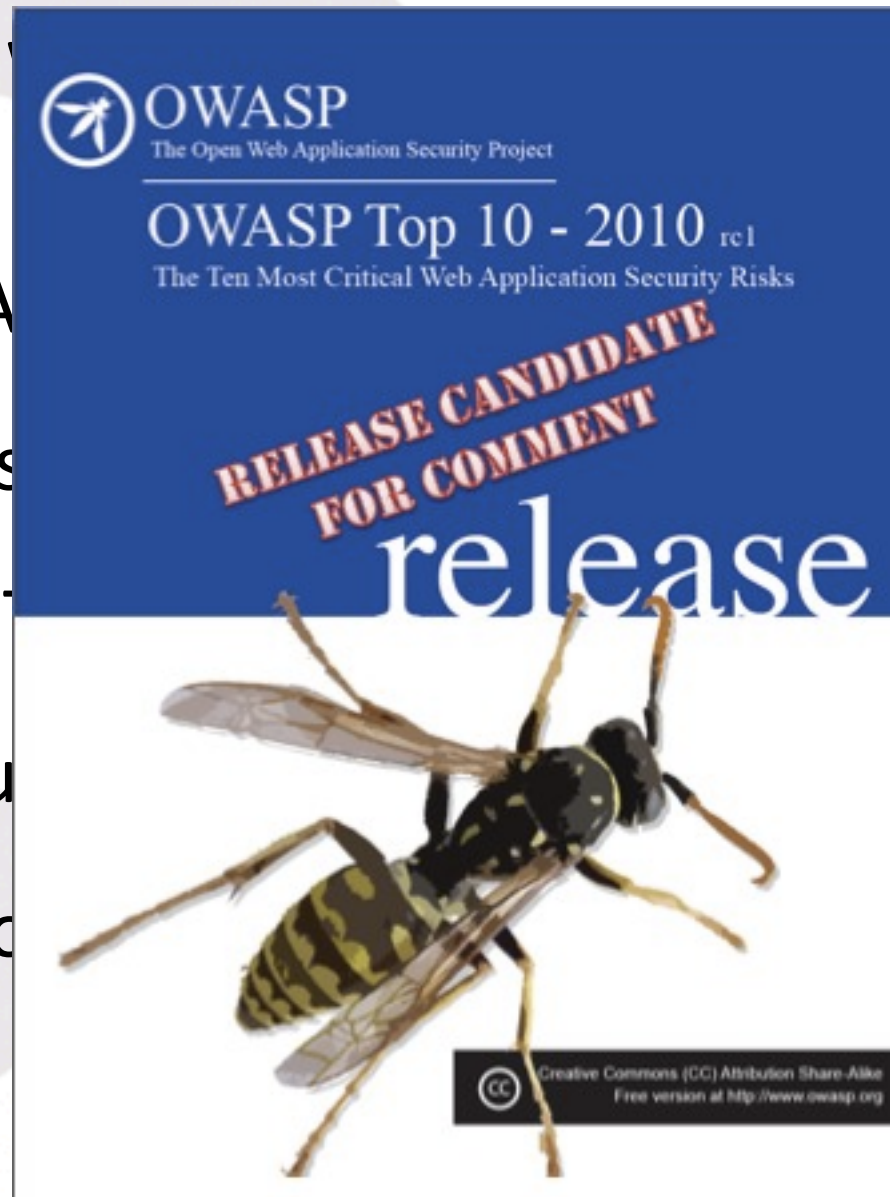
BLUG
Belux Lotus User Group

OWASP

ks

The OWASP
awareness
security.
consensus
application

verful
cation
sents a broad
tical web



OWASP - Top Ten Risks

The OWASP Top Ten provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

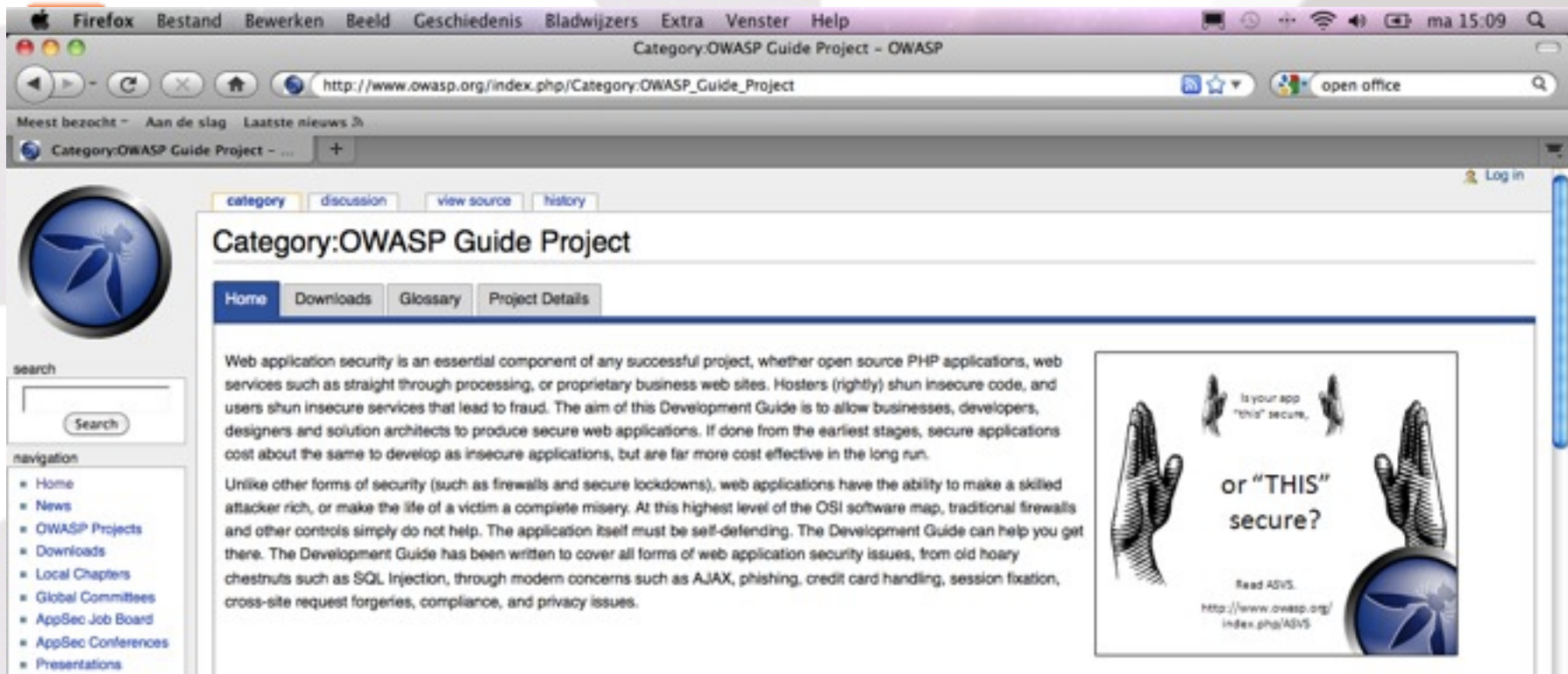
OWASP - Top Ten Risks

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	A7 – Failure to Restrict URL Access
<not in T10 2007>	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	A10 – Insufficient Transport Layer Protection
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>



BLUG
Belux Lotus User Group

OWASP - Guide



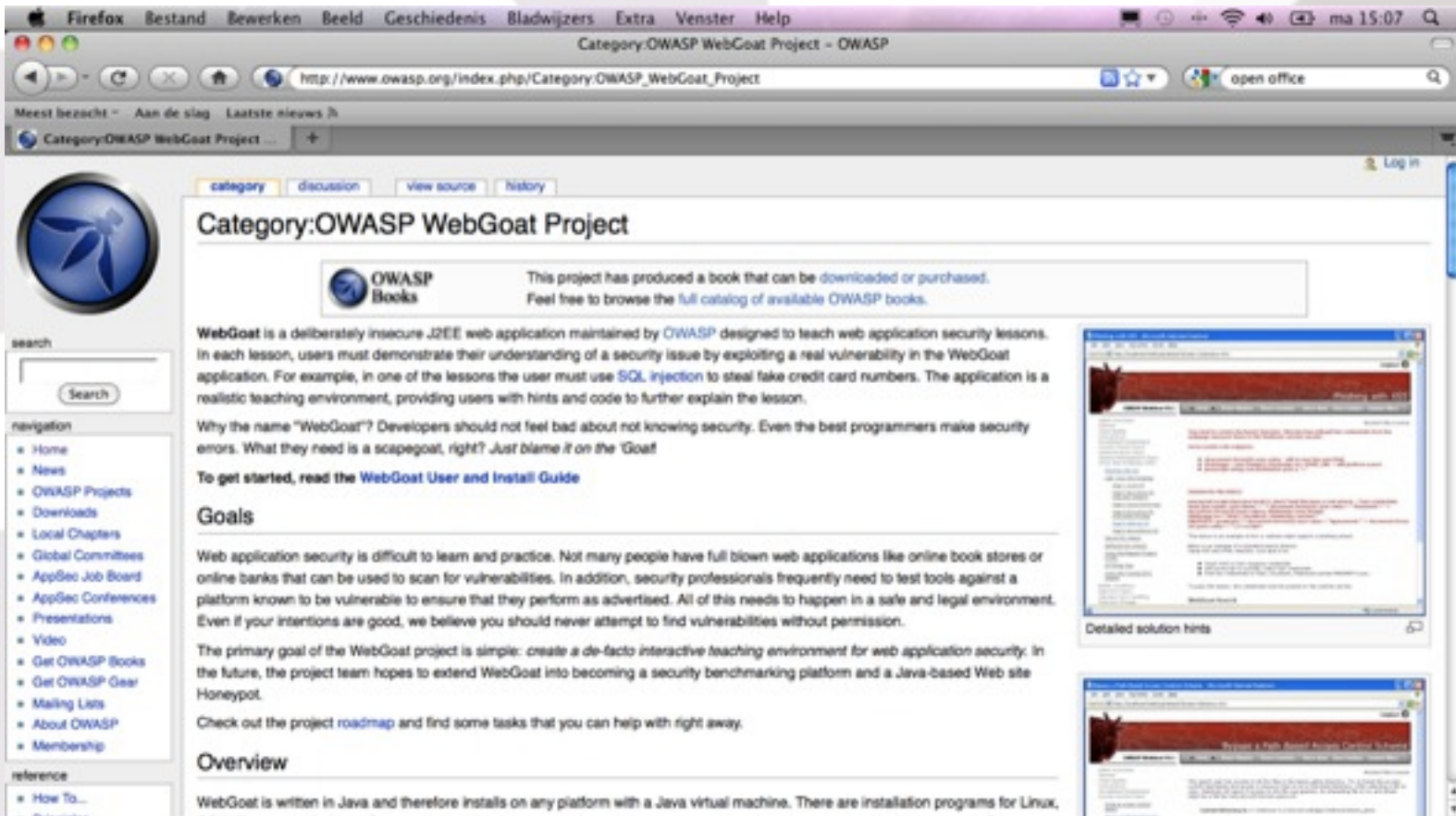
OWASP - Guide

-  Help for All Coders Alike...
-  PHP, Java, C#
-  Examples
-  Hints & Tips



BLUG
Belux Lotus User Group

OWASP - Tools



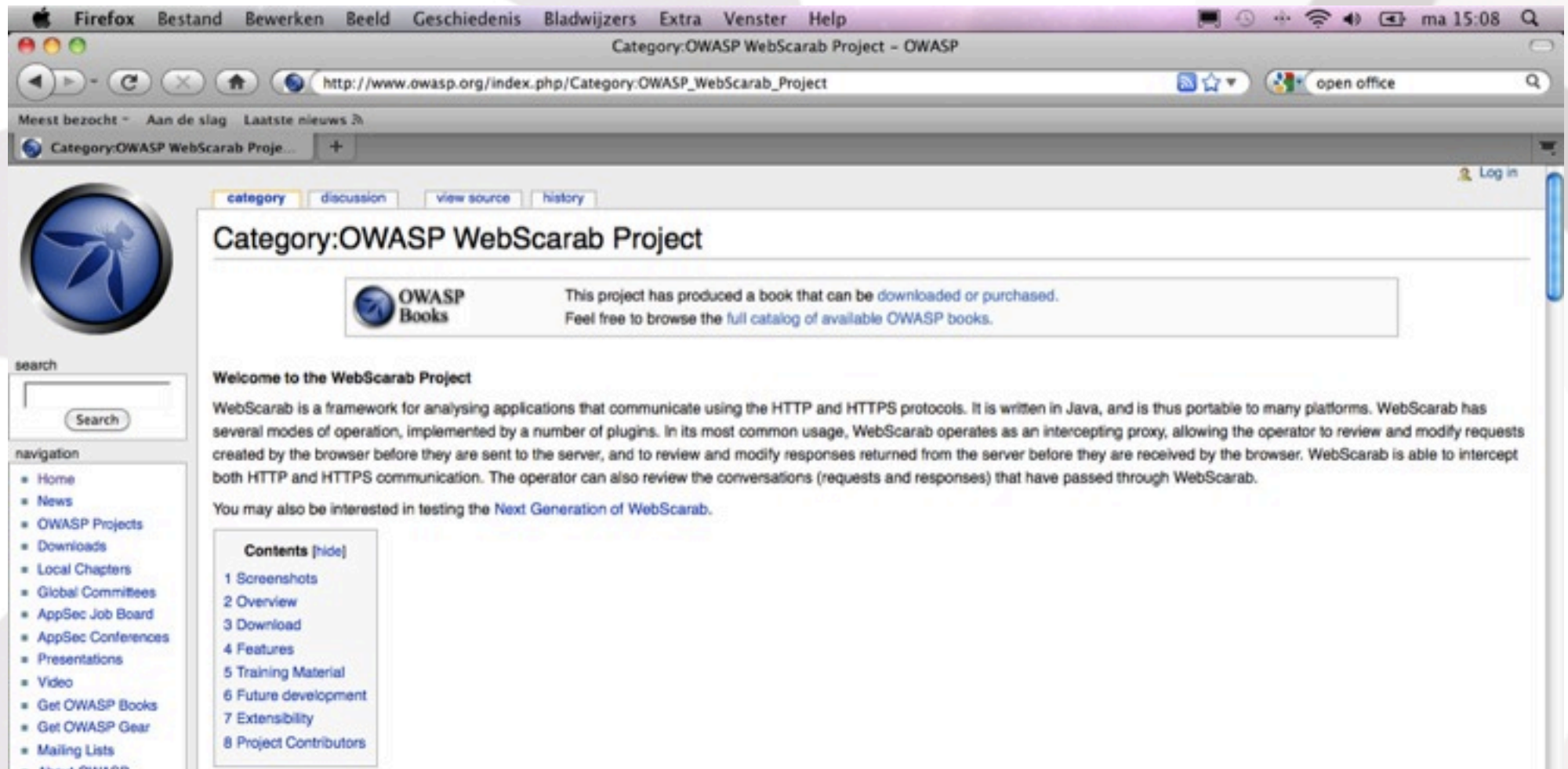
OWASP - Tools

WebGoat is a deliberately insecure J2EE web application maintained by OWASP designed to teach web application security lessons.



BLUG
Belux Lotus User Group

OWASP - Tools



The screenshot shows a Firefox browser window displaying the OWASP WebScarab Project page. The browser's address bar shows the URL http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project. The page title is "Category:OWASP WebScarab Project". The page content includes a welcome message, a description of WebScarab as a framework for analysing applications, and a list of contents. A sidebar on the left contains a search box and a navigation menu. A top banner for OWASP Books is also visible.

Firefox Bestand Bewerken Beeld Geschiedenis Bladwijzers Extra Venster Help ma 15:08

Category:OWASP WebScarab Project - OWASP

[http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project](#)

Meest bezocht - Aan de slag - Laatste nieuws 2h

Category:OWASP WebScarab Proje...

Log in

category discussion view source history

Category:OWASP WebScarab Project

 **OWASP Books** This project has produced a book that can be [downloaded](#) or [purchased](#). Feel free to browse the [full catalog](#) of available OWASP books.

Welcome to the WebScarab Project

WebScarab is a framework for analysing applications that communicate using the HTTP and HTTPS protocols. It is written in Java, and is thus portable to many platforms. WebScarab has several modes of operation, implemented by a number of plugins. In its most common usage, WebScarab operates as an intercepting proxy, allowing the operator to review and modify requests created by the browser before they are sent to the server, and to review and modify responses returned from the server before they are received by the browser. WebScarab is able to intercept both HTTP and HTTPS communication. The operator can also review the conversations (requests and responses) that have passed through WebScarab.

You may also be interested in testing the [Next Generation of WebScarab](#).

Contents [hide]

- 1 Screenshots
- 2 Overview
- 3 Download
- 4 Features
- 5 Training Material
- 6 Future development
- 7 Extensibility
- 8 Project Contributors

search

Search

navigation

- Home
- News
- OWASP Projects
- Downloads
- Local Chapters
- Global Committees
- AppSec Job Board
- AppSec Conferences
- Presentations
- Video
- Get OWASP Books
- Get OWASP Gear
- Mailing Lists

OWASP - Tools

WebScarab is a framework for analysing applications that communicate using the HTTP and HTTPS protocols. WebScarab operates as an intercepting proxy, allowing the operator to review and modify requests.



BLUG
Belux Lotus User Group

OWASP - Models, Techniques & Frameworks

- ESAPI, Enterprise Security API
For Retrofitting Security in Existing Apps
- SAMM, Software Assurance Maturity Model
- ASVS, Application Security Verification Standard

Conclusions

- Everybody makes mistakes, Solve Them, Learn from Them
- Always Evaluate Cost of Mitigation
- Test!

Questions?



BLUG
Belux Lotus User Group

Who is Ferdinand



BLUG
Belux Lotus User Group



Toolzzz...



Paros Proxy:

<http://www.parosproxy.org/>



OWASP:

<http://www.owasp.org>



For Mac Fans:

<http://research.corsaire.com/tools/>



BLUG
Belux Lotus User Group