Webseclab

Elie Bursztein    Baptiste Gourdin    Celine Fabry    Jason Bau    Gustav Rydstedt
Hristo Bojinov    Dan Boneh    John C. Mitchell
Stanford University
Evolution of the number of vulnerabilities by years

- **Web**
- **System**

<table>
<thead>
<tr>
<th>Year</th>
<th>Web</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>1095</td>
<td>1095</td>
</tr>
<tr>
<td>2006</td>
<td>2793</td>
<td>2000</td>
</tr>
<tr>
<td>2007</td>
<td>1951</td>
<td>1528</td>
</tr>
<tr>
<td>2008</td>
<td>996</td>
<td>1531</td>
</tr>
<tr>
<td>2009</td>
<td>1275</td>
<td>1647</td>
</tr>
</tbody>
</table>
Web vulnerabilities breakdown

Evolution of the web vulnerabilities over the years by types

- XSS
- SQLi
- XCS
- Session
- CSRF
- SSL
- Information Leak
BlackHat Training on Web security
No bullet proof language

- php: 5070
- aspx: 1220
- asp: 1170
- jsp: 511
- cfm: 302
- do: 224
- pl: 140
Webseclab Goals

- Blending edge exercises
- Inclusive environment
- No setup
- Minimal learning curve
- Easy class management
Webseclab architecture

Cloud service

User 1
-VM1
-VM2

User 2
-VM1
-VM2
Key features

VM

- Exercises
- Quizzes
- Projects
- Real case

Cloud

- Class management
- Synchronization
- Realtime goal
- Quizzes push
- Analytics
Webseclab’s platform consists of individual virtual-machine environments tied together by a cloud service.

Webseclab combines: - a **cloud service** and - **individual virtual-machine distributions** to provide a web security learning platform that is comprehensive, covering all major security topics deemed important by the security community; contemporary, encompassing recent attacks-and-defenses from hacker conferences and academic research; and tested, used to teach academic courses at **Stanford** and **CMU**.

We undertook the development of Webseclab to address the challenge teaching web application security, which is no easy thing. Web application security is a complex and fast moving target. It covers multiple technologies, e.g. network protocols, cryptographic features, programming languages, across multiple layers, from networks to client/server applications to custom Javascript applets, and it is constantly evolving, with a large number of new vulnerabilities and attacks are uncovered each year. Webseclab, containing over 90 laboratory exercises and provisions for instructor-supplied quizzes and programming projects, represents our best-effort at creating a teaching platform of sufficient scale, that teaches students to appreciate the complexity of the problem yet equipping them with the appropriate solutions.

Each student VM environment contains a large number of focused exercises for learning individual topics, a provision for administering instructor-created quizzes, along with all the software required for completing longer-term security-focused programming projects. The VM offers an all-in-one tool for completing all the teaching material in a package with turn-key installation and an easy-to-use browser-based interface. It also isolates harmful traffic, e.g. those illustrating attacks, keeping them from harming any public or corporate networks. Finally, it is fully integrated and synchronized with the cloud service.

The cloud service features are mainly designed to support class administration, for both instructors and students. Some key features of the cloud include reporting analytics such as progress and grading metrics in both instructor and student views, data backup/migration for individual student VMs, and synchronized project/quiz administration for instructors, including the ability to push new assignments to student VMs.
Quiz Progression for Class blackhat2010

Average score per quiz

Score distribution for Introduction

Select a quiz to display results: Introduction

Students Top 20

Students with difficulties
Webseclab VM architecture

- Virtual Machine
- OS: LINUX
- Database: MySQL
- Web Server: Apache
- Framework: PHP 5
- Exercises: PHP / JS
- Webseclab
Webseclab VM architecture

Webseclab
- Exercises
- Framework
- Web Server
- Database
- OS
- Virtual Machine

Virtual Machine
- IDE
- Sandbox
- Sync
- Dashboard

Firefox
- WebSecLab
  - Exercise
    - Categories
    - Objective
    - Exercise rendered
    - Sync
    - Constraints
    - Exercise code
    - Dashboard
    - Pitch
    - Hints

SQL via phpmyadmin

Elie Bursztein et al
Exercises repartition

- Introduction: 7
- CSRF: 8
- Embedding: 7
- Browser security: 6
- Session: 17
- Phishing: 5
- XSS: 12
- SQL injections: 4
- Authentication: 1

Keywords:
- Browser security
- Session
- Phishing
- Authentication
- Introduction
- CSRF
- Embedding
- XSS
- SQL injections