What is bWAPP?

MME | IT Audits & Security

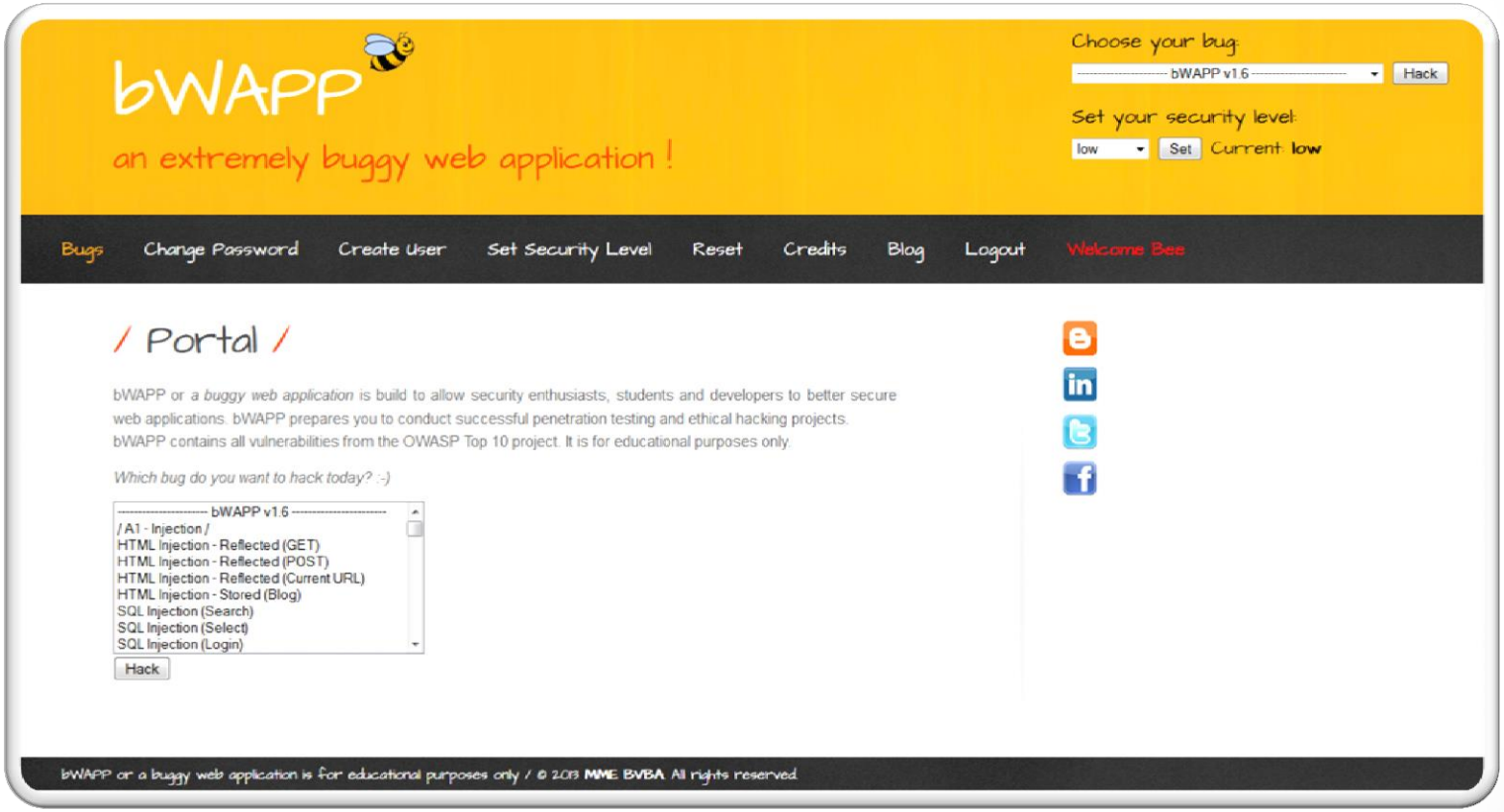
mmeIT
audits & security

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 for successful penetration testing and ethical hacking projects

mmeIT audits & security

bWAPP



mmeIT
audits & security

bWAPP

- 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

bWAPP

- About me

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

mmeIT audits & security

bWAPP

- Architecture
  - Open source PHP application
  - Backend MySQL database
  - Can be hosted on Linux/Windows using Apache/IIS
  - Can be installed with WAMP or XAMPP

bWAPP

- Features
  - Very easy to use and to understand
  - Well structured and documented PHP code
  - Different security levels (low - medium - high)
  - ‘New user’ creation
  - Reset and reinstall database feature
  - Email functionalities
  - ‘Evil’ directory including attack scripts

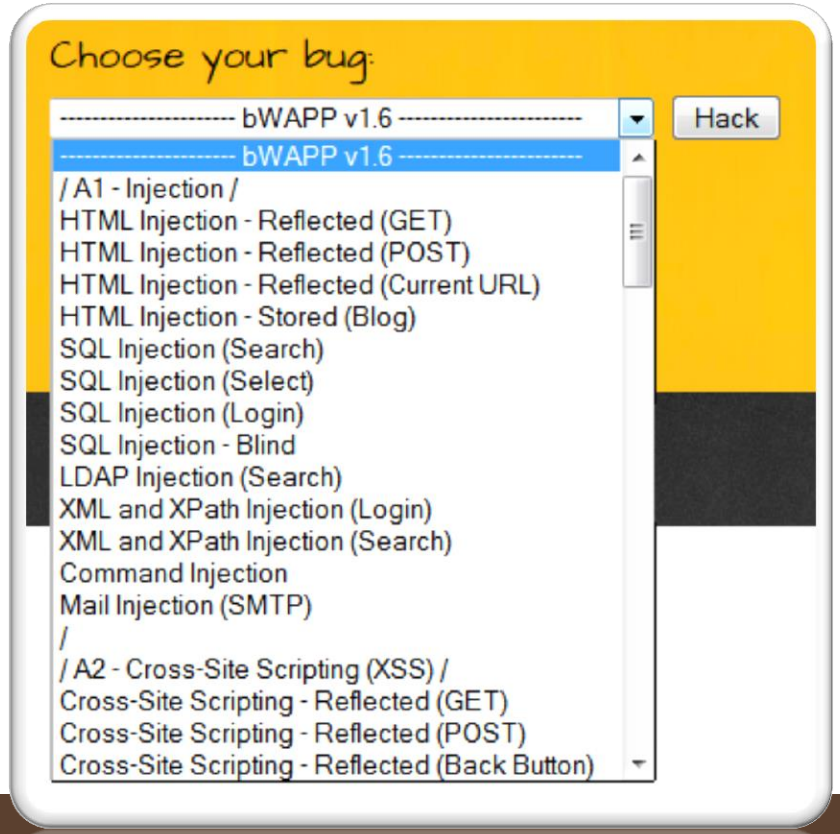
bWAPP

- What makes bWAPP so unique ?
  - Well, it has **over 60** web bugs!
  - Covering all major known web vulnerabilities
  - Including all risks from the OWASP Top 10 project

mmeIT audits & security

bWAPP

- Which bug do you want to hack today ?



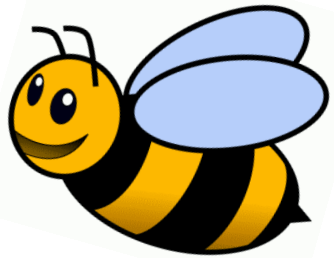
mmeIT audits & security

bWAPP

- Which bug do you want to hack today ? (1)
  - Injection vulnerabilities like SQL, XML/XPath, JSON, LDAP, HTML, Command and SMTP injection
  - Authentication, authorization and session management issues
  - Malicious, unrestricted file uploads
  - Arbitrary file access
  - Directory traversals
  - Local and remote file inclusions (LFI/RFI)
  - Server Side Request Forgery (SSRF)

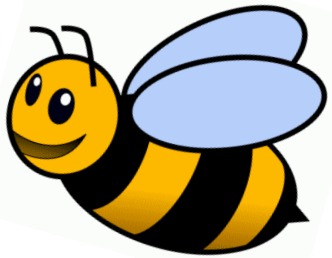
bWAPP

- Which bug do you want to hack today ? (2)
  - Configuration issues: Man-in-the-Middle, Cross-domain policy file, information disclosures,...
  - HTTP parameter pollution and HTTP response splitting
  - Denial-of-Service (DoS) attacks
  - HTML5 ClickJacking, Cross-Origin Resource Sharing (CORS) and web storage issues
  - Unvalidated redirects and forwards
  - Insecure cryptographic storage

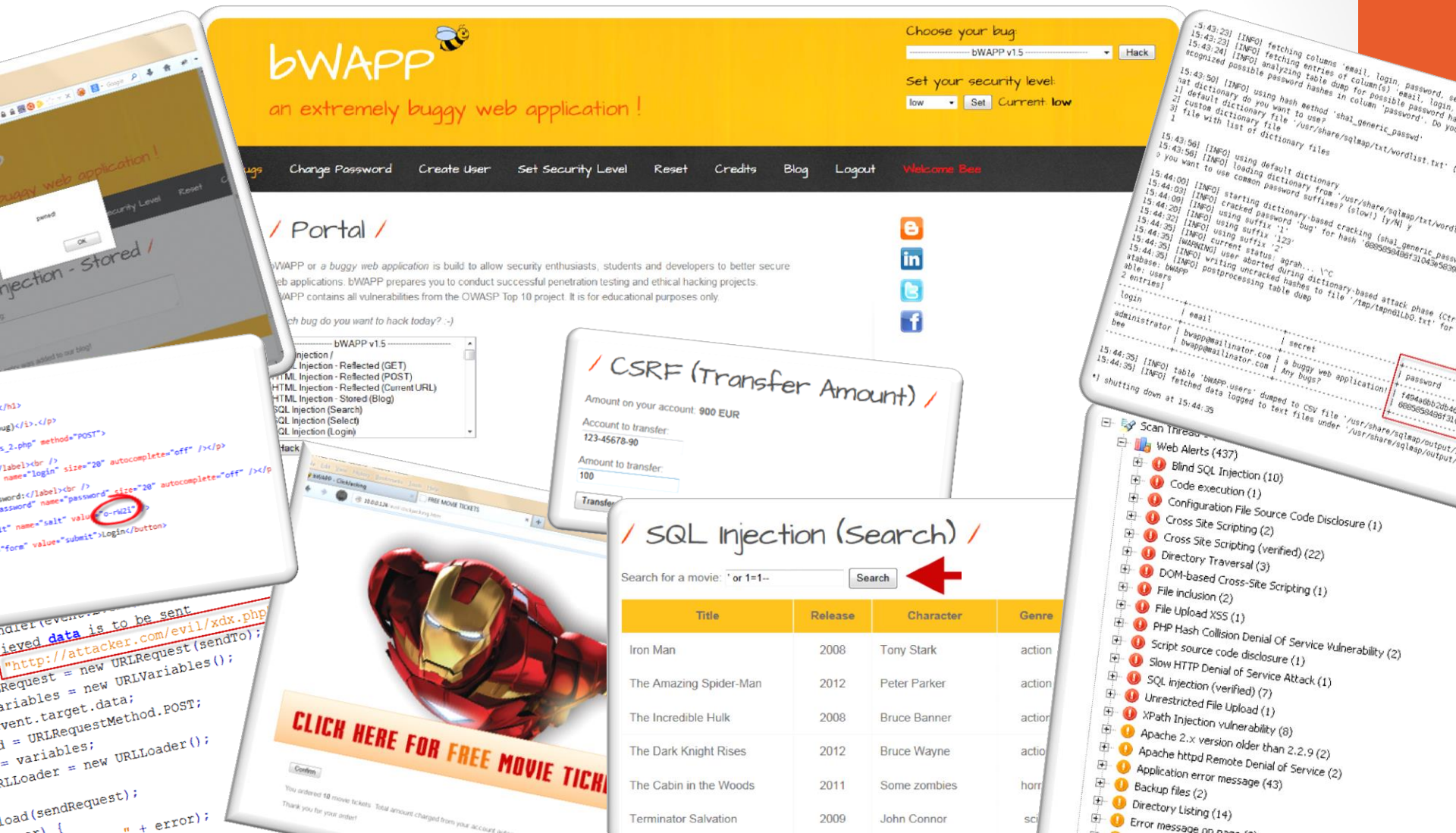


bWAPP

- Which bug do you want to hack today ? (3)
  - Cross-Site Scripting (XSS), Cross-Site Tracing (XST) and Cross-Site Request Forgery (CSRF)
  - Parameter tampering
  - HTTP verb tampering
  - Local privilege escalation
  - AJAX issues
  - And much more ☺

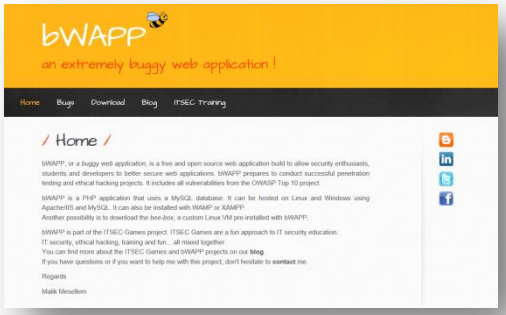


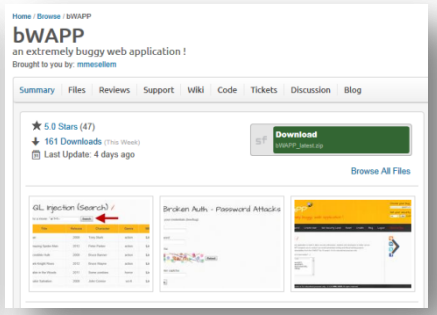
bWAPP


bWAPP
an extremely buggy web application !
Choose your bug:
bWAPP v1.5
Hack
Set your security level:
low
Set
Current: low
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ Portal /
/ CSRF (Transfer Amount) /
Amount on your account: 900 EUR
Account to transfer:
123-45678-90
Amount to transfer:
100
/ 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
The Cabin in the Woods
2011
Some zombies
Terminator Salvation
2009
John Connor
CLICK HERE FOR FREE MOVIE TICK
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)

bWAPP

- External links
  - Home page - www.itsecgames.com
  - Download location - sourceforge.net/projects/bwapp
  - Blog - itsecgames.blogspot.com

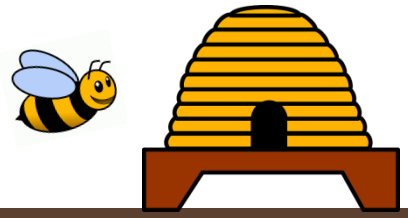




mmeIT audits & security

bee-box

- Meet the **bee-box**… a home for our bee
- VM pre-installed with bWAPP
- LAMP environment: **L**inux, **A**pache, **M**ySQL and **P**HP
- Requires zero installation
  - Made for those who are really lazy ☺
  - Reduces the ‘how to use bWAPP?’ SPAM in my mailbox



bee-box

- bee-box is also made deliberately insecure…
- Gives you several ways to hack and deface bWAPP
  - Even possible to hack the bee-box to get full root access!
- Opportunity to explore all bWAPP vulnerabilities
- Hacking, defacing and exploiting without going to jail
- You can download bee-box from here

bee-box

bee-box

- Features (1)
  - Apache, MySQL and PHP installed and configured
  - phpMyAdmin installed
  - Postfix installed and configured
  - .htaccess files support enabled
  - AppArmor disabled
  - PHP LDAP extension installed

bee-box

- Features (2)
  - ‘Tuned’ file access permissions
  - Configured with a self-signed certificate (SSL)
  - Some basic security tools installed
  - Shortcuts to start, install and update bWAPP
  - An amazing wallpaper :)
  - And last but not least, an outdated Linux kernel…

bWAPP and bee-box

- Both are part of the ITSEC GAMES project
- A fun approach to IT security education
- IT security, ethical hacking, training and fun... all mixed together

bWAPP and bee-box

- Ready, set, and hack !
- There's only 1 thing to remember
- The logon credentials are…

bee/bug

bWAPP and bee-box

- Ready, set, and hack !
- There's only 1 thing to remember
- The logon credentials are **bee/bug**
- So please don't SPAM me anymore

bWAPP and bee-box

- More credentials (for wizkids only)
  - bWAPP
    - bee/bug
  - bee-box
    - bee/bug
    - Super user: bug
  - MySQL and phpMyAdmin
    - root/bug

bWAPP and bee-box

- Installation and configuration
  - Install VMware Player, Workstation or Fusion
  - Install and start the bee-box VM
  - Configure or check the IP settings
  - Browse to the bWAPP web app
    - http://[IP]/bWAPP/
  - Login with **bee/bug**

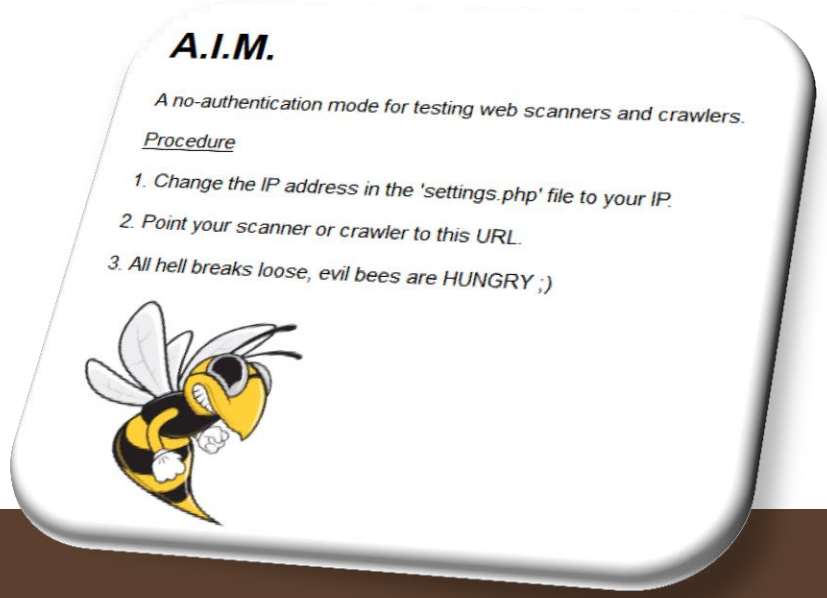
bWAPP and bee-box

- Settings
  - General application settings
    - sudo gedit /var/www/bWAPP/admin/settings.php

```
// A.I.M., a no-authentication mode for testing web scanners and crawlers
// Evil bees are HUNGRY ;)
// URL: http://itsecgames.com/bWAPP/aim.php
$remote_IP = "6.6.6.6";

// Credentials, used on some pages
$login = "bee";
$password = "bug";
```

bWAPP and bee-box

- A.I.M.
  - No-authentication mode
  - For testing web scanners and crawlers
    - http://[IP]/bWAPP/aim.php



mmeIT audits & security

bWAPP and bee-box

- Reset options
  - Resets the application
    - http://[IP]/bWAPP/reset.php
  - Resets the application + database
    - http://[IP]/bWAPP/reset.php?secret=bWAPP

bWAPP and bee-box

- Host file (optional)
  - Change the host file on the local machine

mmeIT audits & security

bWAPP and bee-box

- Postfix (optional)
  - Reconfigure and restart Postfix on the bee-box
    - sudo gedit /etc/postfix/main.cf

      sudo /etc/init.d/postfix restart

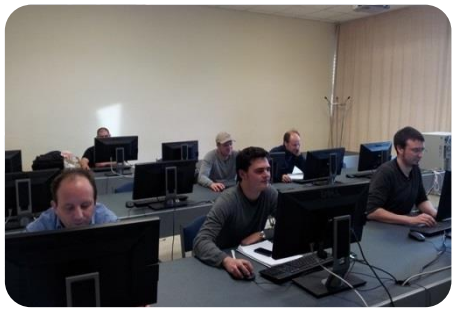
```
myhostname = bee-box
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = itsecgames.com, bee-box, localhost.localdomain, localhost

# Replace the hostname with the hostname of YOUR SMTP provider :)
relayhost = out.telenet.be

mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
```

Training and workshop

- Attacking & Defending Web Apps with bWAPP
  - 2-day comprehensive web security course
  - More info: http://goo.gl/ASuPa1 (pdf)
- Plant the Flags (PTF) with bWAPP
  - 4-hour web security workshop
  - Perfect for your conference or group event!
  - More info: http://goo.gl/fAwCex (pdf)

mmeIT audits & security

Training and workshop






mmeIT
audits & security

Contact me

- Thanks!

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

mmeIT audits & security