



What is **bWAPP**?

MME | IT Audits & Security




bWAPP == extremely buggy

- bWAPP, or a **b**uggy **W**eb **A**PPlication
- 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



bWAPP

The screenshot shows the bWAPP web application interface. The header is yellow with the bWAPP logo and a bee icon. Below the logo is the text "an extremely buggy web application!". On the right, there are two sections: "Choose your bug:" with a dropdown menu showing "bWAPP v1.6" and a "Hack" button, and "Set your security level:" with a dropdown menu showing "low", a "Set" button, and the text "Current: low". Below the header is a dark navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. The main content area has a heading "/ Portal /" and a paragraph explaining that bWAPP is a buggy web application built for security enthusiasts, students, and developers to better secure web applications. It mentions that bWAPP prepares users to conduct successful penetration testing and ethical hacking projects and contains all vulnerabilities from the OWASP Top 10 project. Below this is a question "Which bug do you want to hack today? :-)" and a list of bugs in a dropdown menu: /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), and SQL Injection (Login). There is a "Hack" button below the list. On the right side of the main content area, there are social media icons for e, in, t, and f. At the bottom, there is a footer with the text "bWAPP or a buggy web application is for educational purposes only / © 2013 MME BVBA. All rights reserved."

bWAPP 

an extremely buggy web application !

Choose your bug:
bWAPP v1.6 Hack

Set your security level:
low Set Current: low

Bugs 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 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 v1.6

- /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)

Hack

e in t f

bWAPP or a buggy web application is for educational purposes only / © 2013 MME BVBA. All rights reserved.

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



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



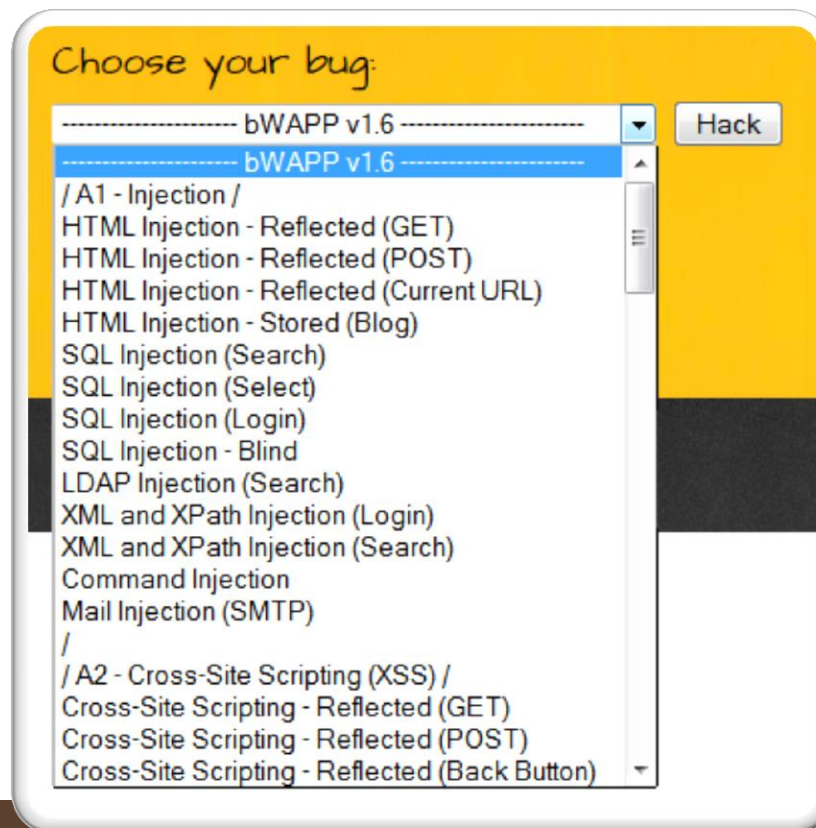
bWAPP

- 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



bWAPP

- Which bug do you want to hack today ?



bWAPP

- Which bug do you want to hack today ? (1)
 - Injection vulnerabilities like SQL, XML/XPath, LDAP, HTML, Command and SMTP injection
 - Cross-Site Scripting (XSS), Cross-Site Tracing (XST) and Cross-Site Request Forgery (CSRF)
 - Authentication, authorization and session management issues
 - Malicious, unrestricted file uploads
 - Arbitrary file access and directory traversals
 - Local and remote file inclusions (LFI/RFI)
 - Parameter tampering

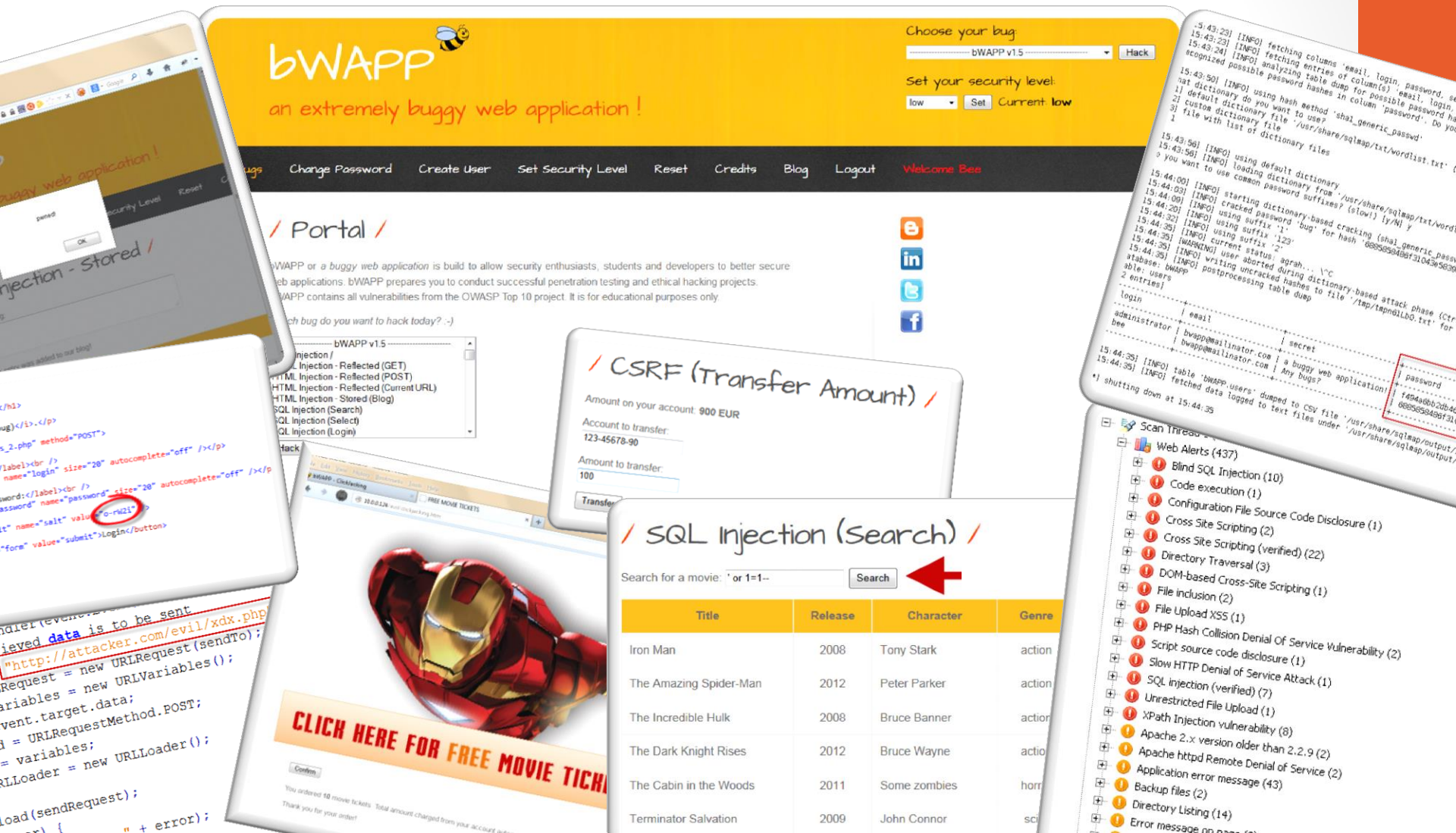


bWAPP

- 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
 - And much more 😊



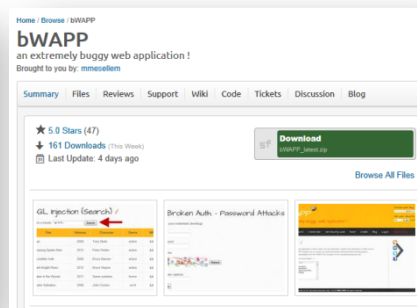
bWAPP



bwAPP

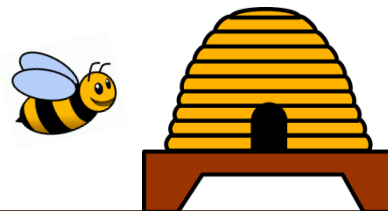
■ External links

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



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@bee-box: /var/www/bWAPP
File Edit View Terminal Tabs Help
bee@bee-box:/var/www/bWAPP$ ls
at_restrict_device_access.php      ldapi.php
at_restrict_folder_access.php      login.php
ba_forgotten.php                  logout.php
ba_insecure_login_1.php            maili.php
ba_insecure_login_2.php            message.txt
ba_insecure_login_3.php            mysqli_ps.php
ba_insecure_login.php              password_change.php
ba_logout_1.php                    password
ba_logout.php                      php_eval.php
ba_pwd_attacks_1.php               phpinfo.php
ba_pwd_attacks_2.php               portal.php
ba_pwd_attacks_3.php               reset.php
ba_pwd_attacks_4.php               rlfi.php
ba_pwd_attacks.php                 robots.txt
bugs.txt                           secret_change.php
captcha_box.php                    secret-cors-1.php
captcha.php                        secret-cors-2.php
clickjacking.php                   secret-cors-3.php
commandi.php                       secret.php
config.inc                         security_level_check.php
config.inc.php                     security_level_set.php
config.inc.php~                    security.php
connect.i.php                       selections.php
```


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

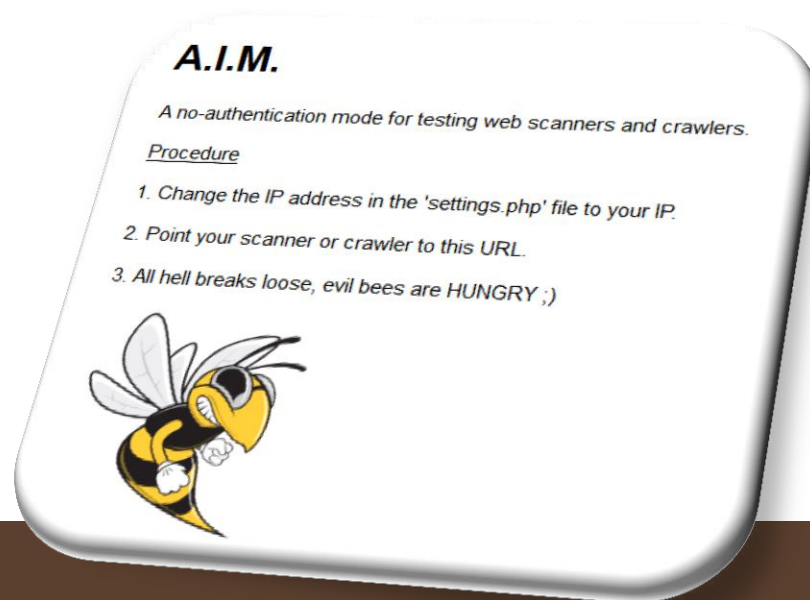
- Settings
 - General application settings
 - `sudo gedit /var/www/bWAPP/admin/settings.php`

```
// 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](http://[IP]/bWAPP/aim.php)



bWAPP and bee-box

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

bWAPP and bee-box

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

```
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com          # x client host
# localhost name resolution is handled within DNS itself.
#      127.0.0.1        localhost
#      ::1              localhost
# Replace 10.0.1.51 with YOUR bee-box IP :)
10.0.1.51      itsecgames.com
10.0.1.51      intranet.itsecgames.com
10.0.1.51      attacker.com
```

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

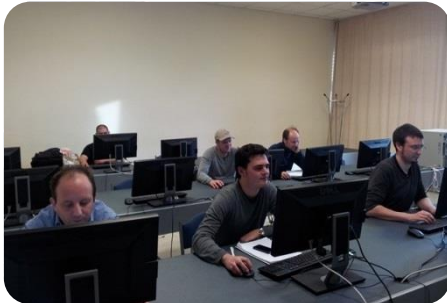
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
```

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)



Training



Contact me

■ Thanks!

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

