Attack your Site for Defense

An introduction to identifying website vulnerabilities with user friendly tools.

OWASP Chapter at UW Bothell
The Gray Hats Team at UW Bothell

www.owasp.org/index.php/UW_Bothell
orgsync.com/81448/chapter (student club)

David L. Morse
linkedin.com/in/davidlmorse

UWB Gray(ish) Hats

- Student cyber defense team
- Gathering together people interested in securing stuff by breaking it
- No experience needed; new members always welcome!
- To learn more, contact Brendan Sweeney: bps7@uw.edu

http://www.nationalccdc.org/

The Problem

- Websites are continuously, actively attacked via automated tools, botnets, and monsters !!!
- Rapid changes in tech + increasing complexity = devs struggle to stay current
- Given time, attackers will Always Win

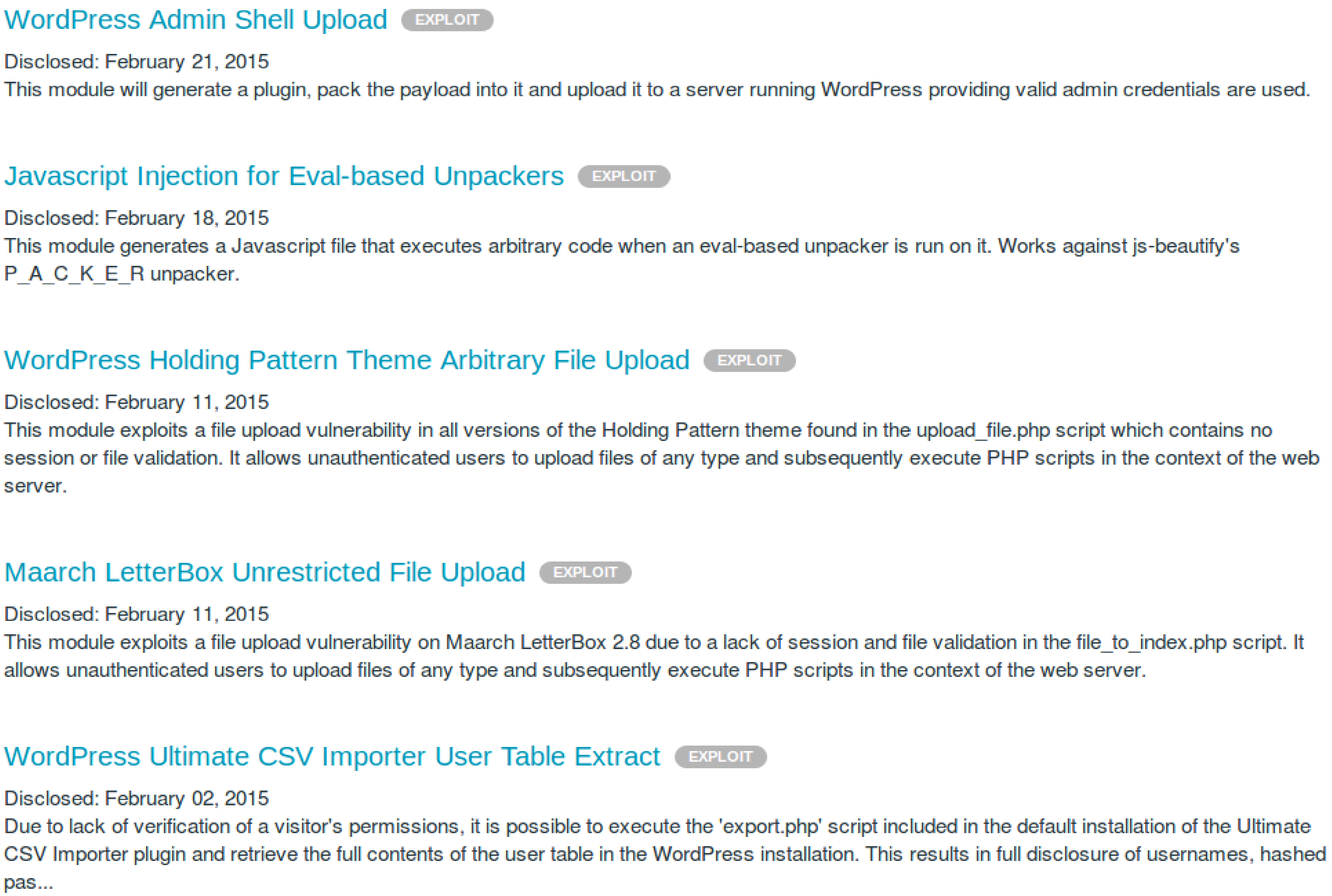
http://www.pcworld.com/article/2045282/microsoft-almost-90-percent-of-citadel-botnets-in-the-world-disrupted-in-june.html

http://galleryhip.com/computer-hacker-icon.html

Damn Kids !!!

- Modern tools make vuln discov and pen easy
- Burp Suite, Metasploit, Armitage, Grabber, Vega, Wapiti, etc, etc...
- Suites of tools make "hail Mary" attacks possible (although noisy) by un-trained
  - can damage network devices (even if don't pen)
  - can cause DOS
  - have low cost to attacker
  - likely kids successful against weak / non-current sys (eg. if your web-app is vulnerable or admin lazy)

Example: Most recent Metasploit modules



WordPress Admin Shell Upload EXPLOIT

Disclosed: February 21, 2015

This module will generate a plugin, pack the payload into it and upload it to a server running WordPress providing valid admin credentials are used.

Javascript Injection for Eval-based Unpackers EXPLOIT

Disclosed: February 18, 2015

This module generates a Javascript file that executes arbitrary code when an eval-based unpacker is run on it. Works against js-beautify's P_A_C_K_E_R unpacker.

WordPress Holding Pattern Theme Arbitrary File Upload EXPLOIT

Disclosed: February 11, 2015

This module exploits a file upload vulnerability in all versions of the Holding Pattern theme found in the upload_file.php script which contains no session or file validation. It allows unauthenticated users to upload files of any type and subsequently execute PHP scripts in the context of the web server.

Maarch LetterBox Unrestricted File Upload EXPLOIT

Disclosed: February 11, 2015

This module exploits a file upload vulnerability on Maarch LetterBox 2.8 due to a lack of session and file validation in the file_to_index.php script. It allows unauthenticated users to upload files of any type and subsequently execute PHP scripts in the context of the web server.

WordPress Ultimate CSV Importer User Table Extract EXPLOIT

Disclosed: February 02, 2015

Due to lack of verification of a visitor's permissions, it is possible to execute the 'export.php' script included in the default installation of the Ultimate CSV Importer plugin and retrieve the full contents of the user table in the WordPress installation. This results in full disclosure of usernames, hashed pas...

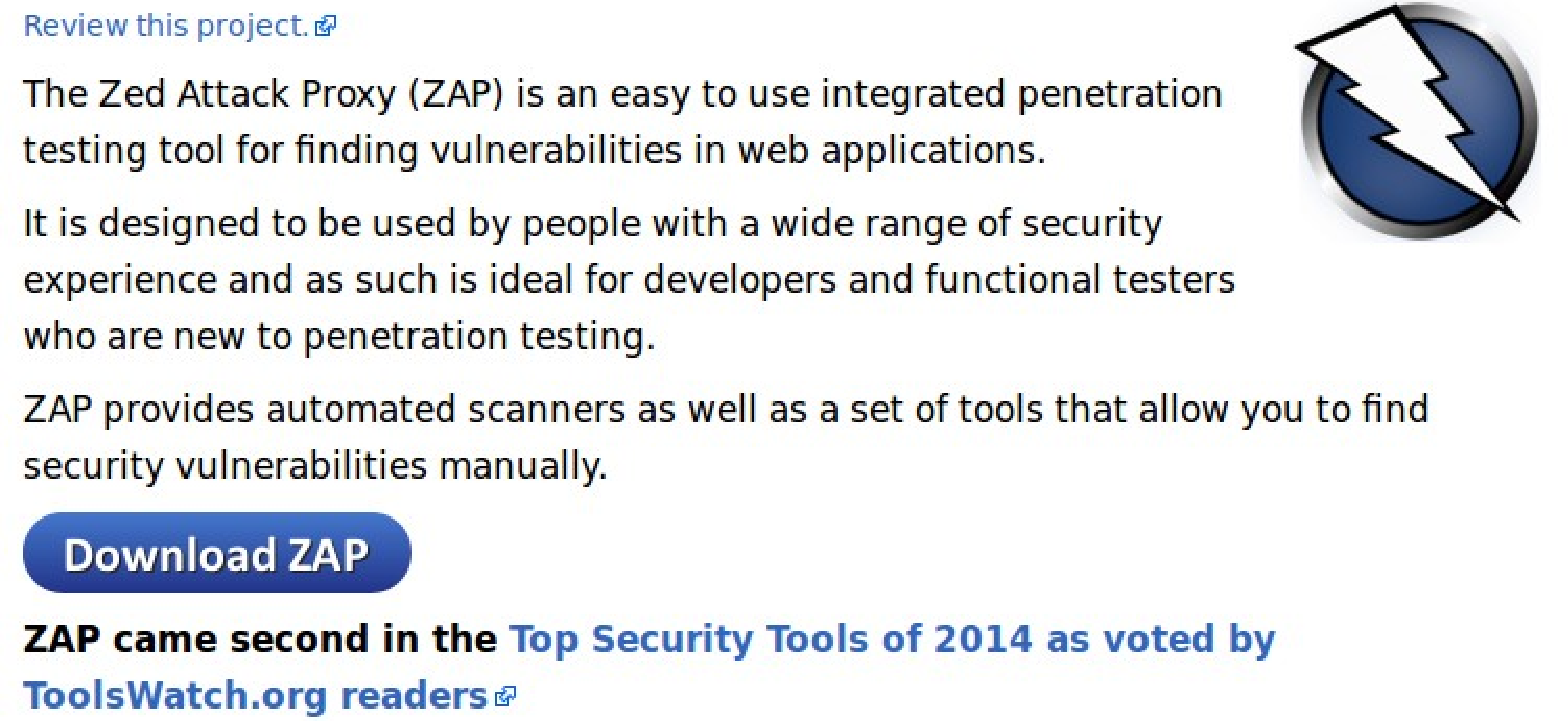
http://www.rapid7.com/db/modules/

The Goal

- Developers need help, let's share best practice
- User friendly tools exist !!!

- Let's have fun, learn defensive coding and secure the WEB :-)

Today's Tool   (no, it's not dave...)



Review this project.

The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

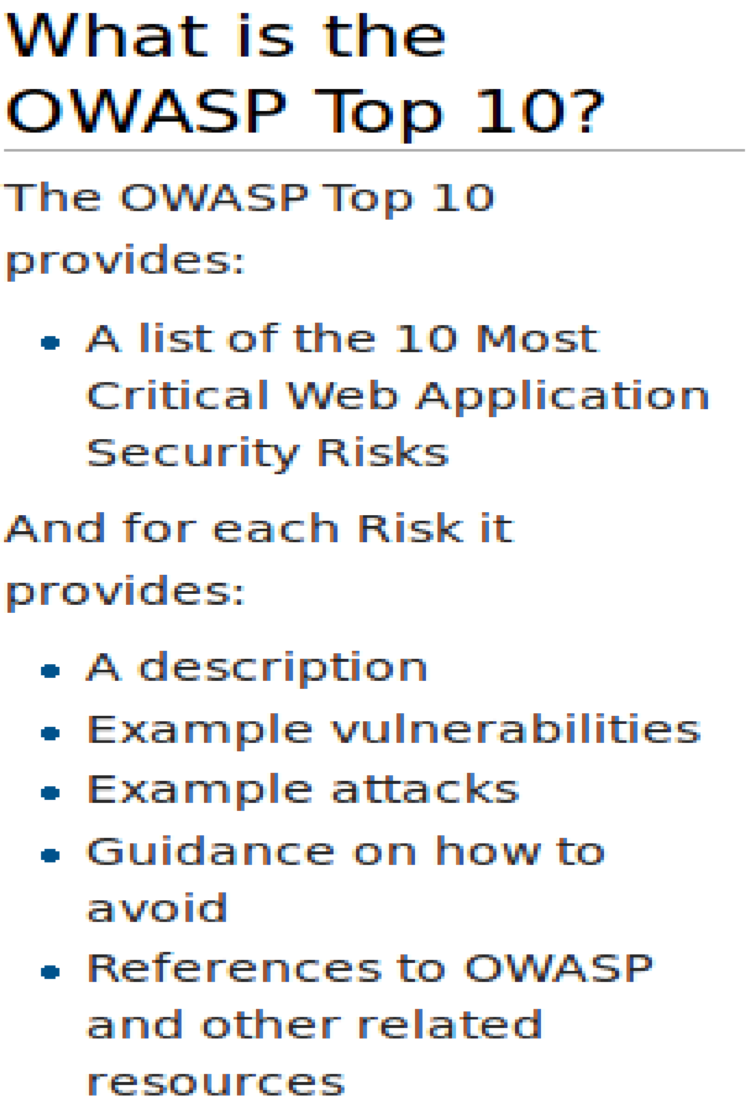
It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing.

ZAP provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.

ZAP came second in the Top Security Tools of 2014 as voted by ToolsWatch.org readers

https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

OWASP == Sexy++



What is the OWASP Top 10?

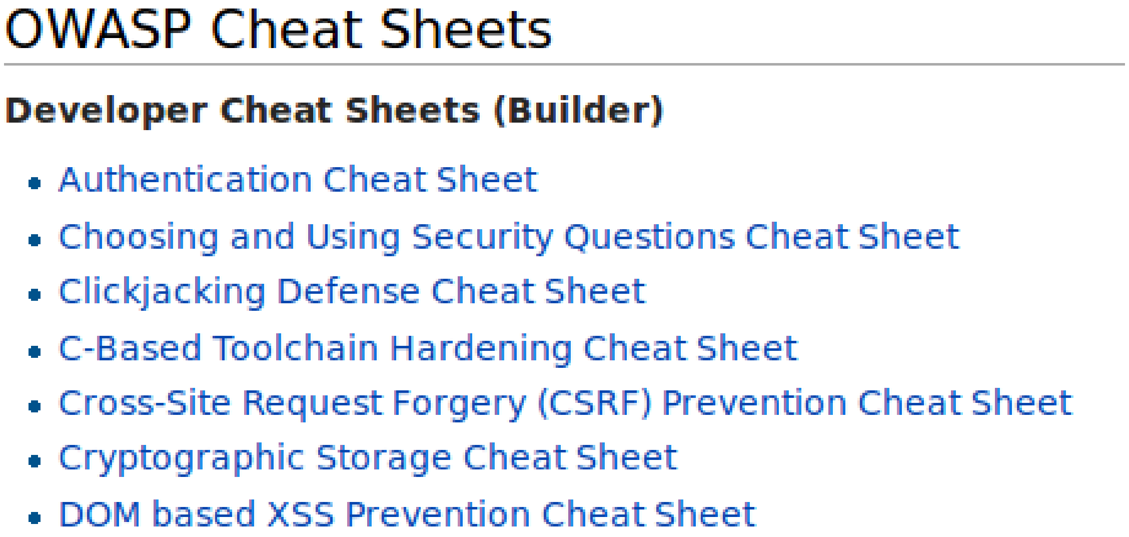
The OWASP Top 10 provides:

- A list of the 10 Most Critical Web Application Security Risks

And for each Risk it provides:

- A description
- Example vulnerabilities
- Example attacks
- Guidance on how to avoid
- References to OWASP and other related resources

The OWASP Testing Guide includes a "best practice" ... techniques for testing most common web application and web service security issues.



OWASP Cheat Sheets

Developer Cheat Sheets (Builder)

- Authentication Cheat Sheet
- Choosing and Using Security Questions Cheat Sheet
- Clickjacking Defense Cheat Sheet
- C-Based Toolchain Hardening Cheat Sheet
- Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet
- Cryptographic Storage Cheat Sheet
- DOM based XSS Prevention Cheat Sheet

owasp.org/index.php/Cheat_Sheets

Setup a testing environment

- install vmware player (or virtual box, etc.)

  (for this demo, example platform host Linux Mint)

- download the latest tar.gz of the bundle from:

  https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/7_0

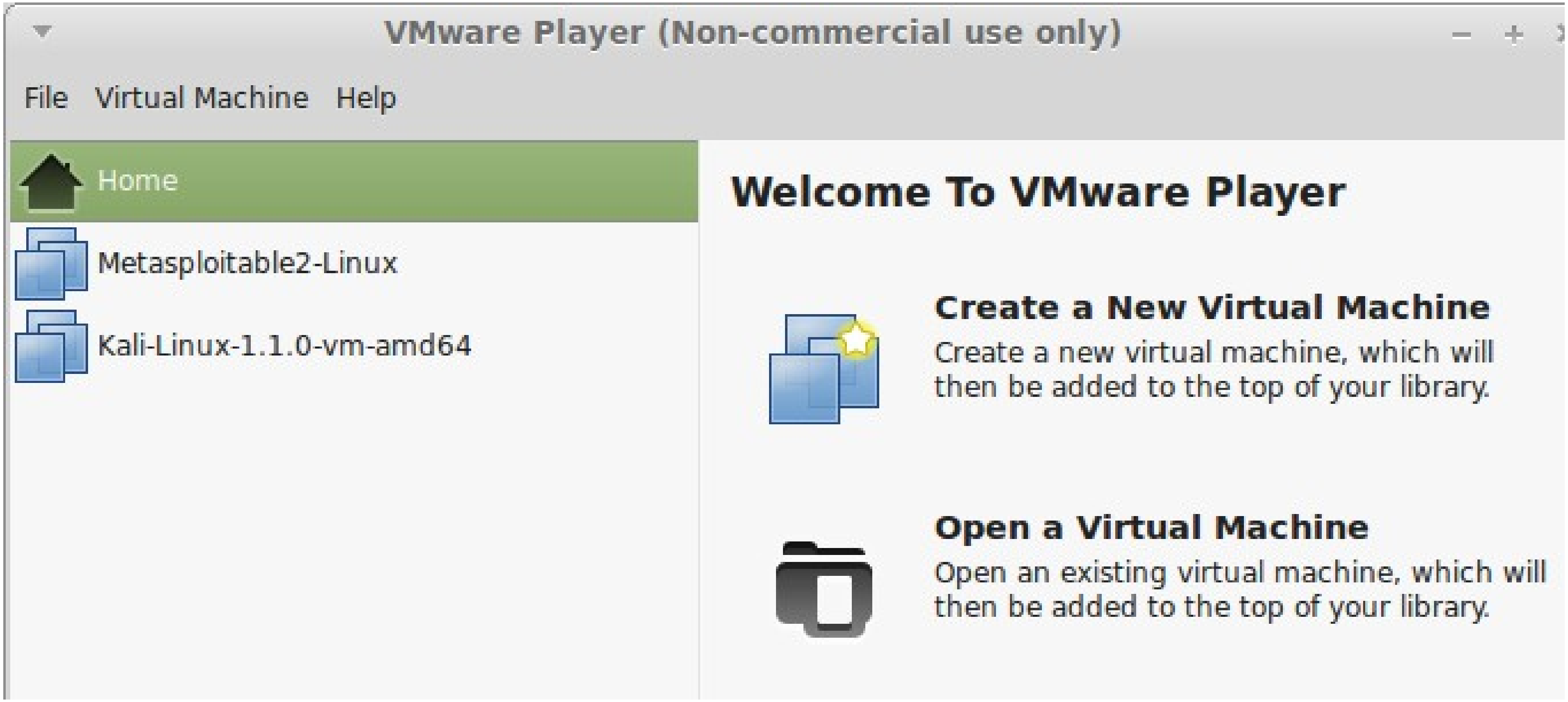
- Install via:

  gksudo bash ~/Downloads/VMware-Player-7.1.0-2496824.x86_64.bundle

- Note - we will isolate!!! the setup

  to protect the innocent

Simple Virt Environ



VMware Player (Non-commercial use only)

Welcome To VMware Player

Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.

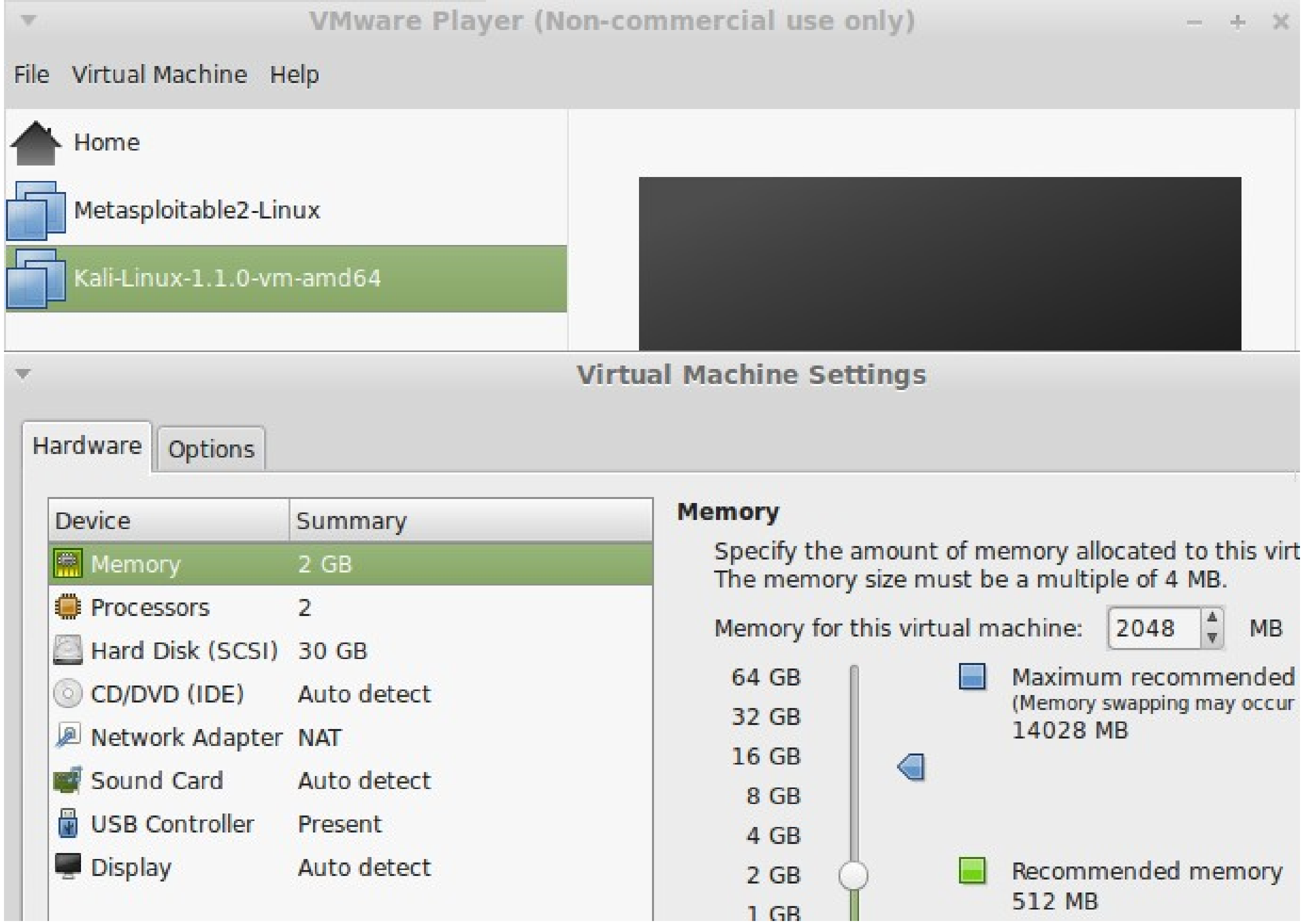
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.

Install the Attacker Guest

- install a kali vm (could use ISO, we use VM-image)
  - kali is based on Debian Linux
  - defaults to "root" user, use caution !!!!
- download the latest vm image from:

  https://www.offensive-security.com/kali-linux-vmware-arm-image-download/
- Make some changes:
  - add user + sudo
  - change root pass
  - do updates (apt-get update & upgrade)

Kali Settings



Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	30 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
Sound Card	Auto detect
USB Controller	Present
Display	Auto detect

Memory

Specify the amount of memory allocated to this virt
The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 2048 MB

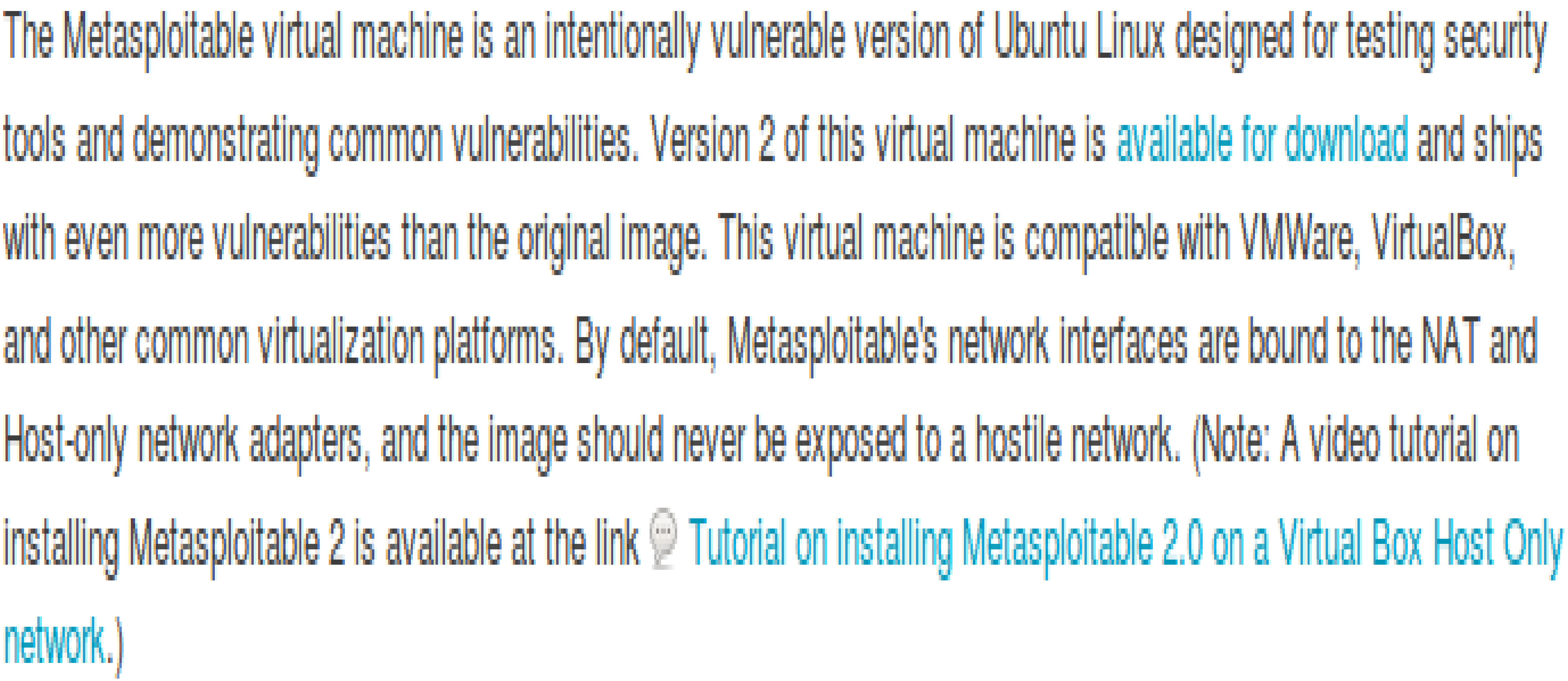
🟦 Maximum recommended
(Memory swapping may occur
14028 MB

🟩 Recommended memory
512 MB

About the Victim

- Metasploitable 2 Exploitability Guide

  https://community.rapid7.com/docs/DOC-1875



The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. Version 2 of this virtual machine is available for download and ships with even more vulnerabilities than the original image. This virtual machine is compatible with VMWare, VirtualBox, and other common virtualization platforms. By default, Metasploitable's network interfaces are bound to the NAT and Host-only network adapters, and the image should never be exposed to a hostile network. (Note: A video tutorial on installing Metasploitable 2 is available at the link Tutorial on installing Metasploitable 2.0 on a Virtual Box Host Only network.)

Install Victim VM

- install the metasploitable vm

  download image (latest is 2012) sourceforge (or goog):

  http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

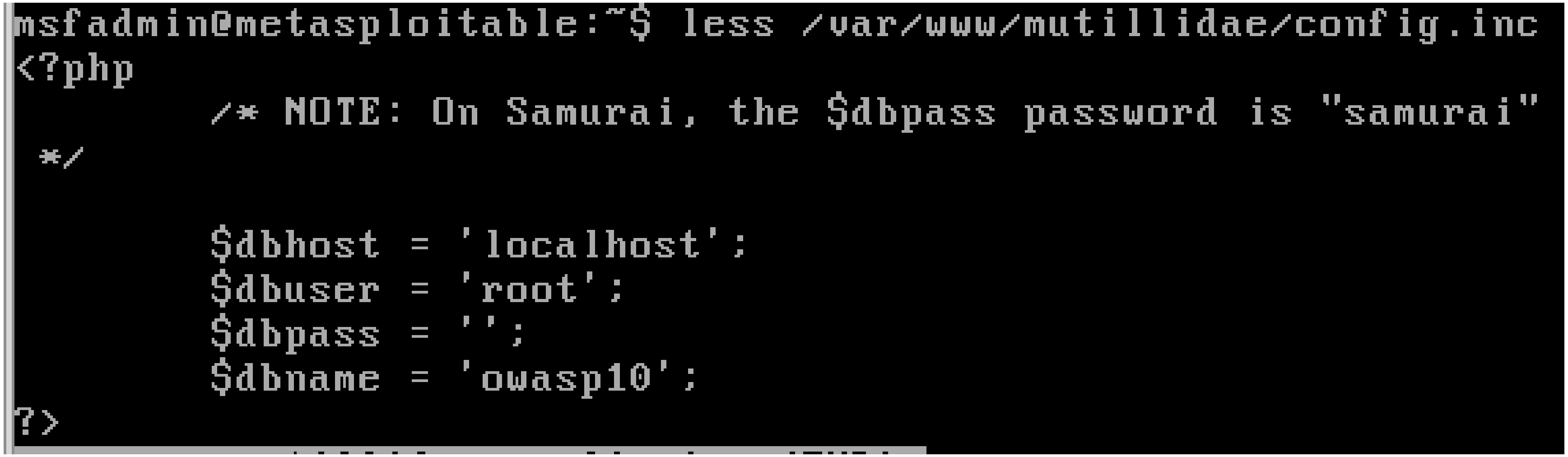
- **** Secure the host Network ****
  - Airgap, firewall, NAT, harden, change users/passes
  - do NOT let Victim image connect to internet !!!!
  - do NOT scan while Attacker connected to internet !!!!

Metasplotable2 - Willing Victim

- metasploitable default login and password

  msfadmin : msfadmin

- tweak (no, not twerk) to the DB name:
  - currently metasploit, change to "owasp10"
  - sudo vi /var/www/mutillidae/config.inc



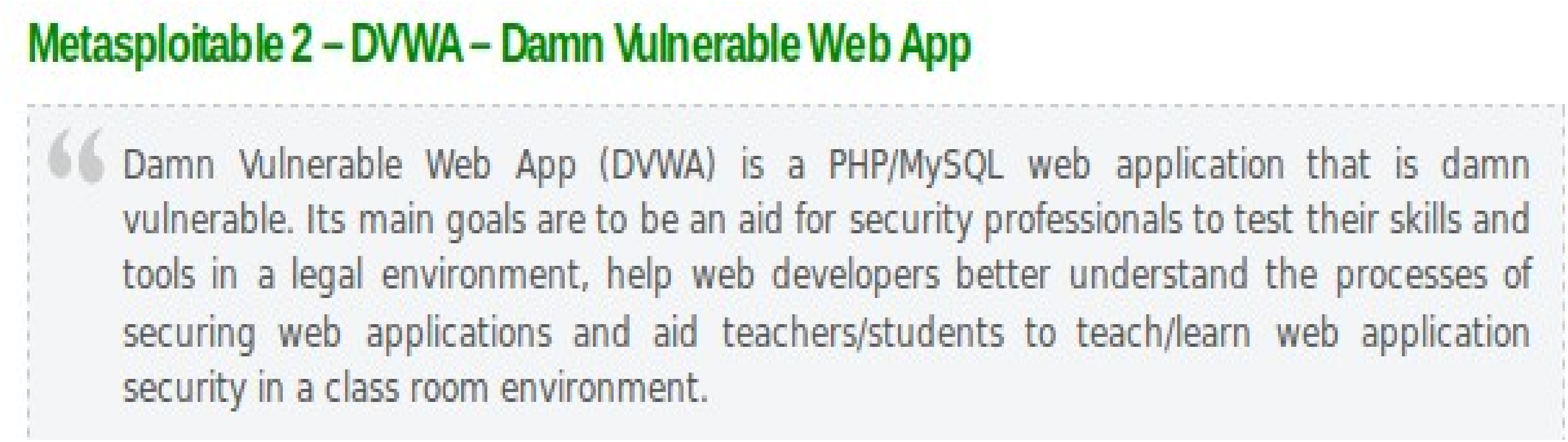
```
msfadmin@metasploitable:~$ less /var/www/mutillidae/config.inc
<?php
        /* NOTE: On Samurai, the $dbpass password is "samurai"
 */

        $dbhost = 'localhost';
        $dbuser = 'root';
        $dbpass = '';
        $dbname = 'owasp10';
?>
```

Finding it

- scan ports
  - use "ifconfig" (or "ip addr") to show victim IP
  - use nmap to scan for open ports:
    - nmap -p0-65535 192.168.x.x
- applications are installed in Metasploitable 2 in the /var/www directory
  - usd "ls /var/www" to view the directory
- Cool stuff - PHP information disclosure page can be found by browsing from the attacking machine:
  - http://192.168.x.x/phpinfo.php

    (wow!! this shouldn't be visible to a visitor !!)



Metasploitable 2 – DVWA – Damn Vulnerable Web App

> Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

DVWA - Damn Vulnerable Web App.

Default username = admin
Default password = password

Accessing the Victim Website

The Mutillidae web application (NOWASP (Mutillidae)) contains all of the vulnerabilities from the OWASP Top Ten plus a number of other vulnerabilities such as HTML-5 web storage, forms caching, and click-jacking.

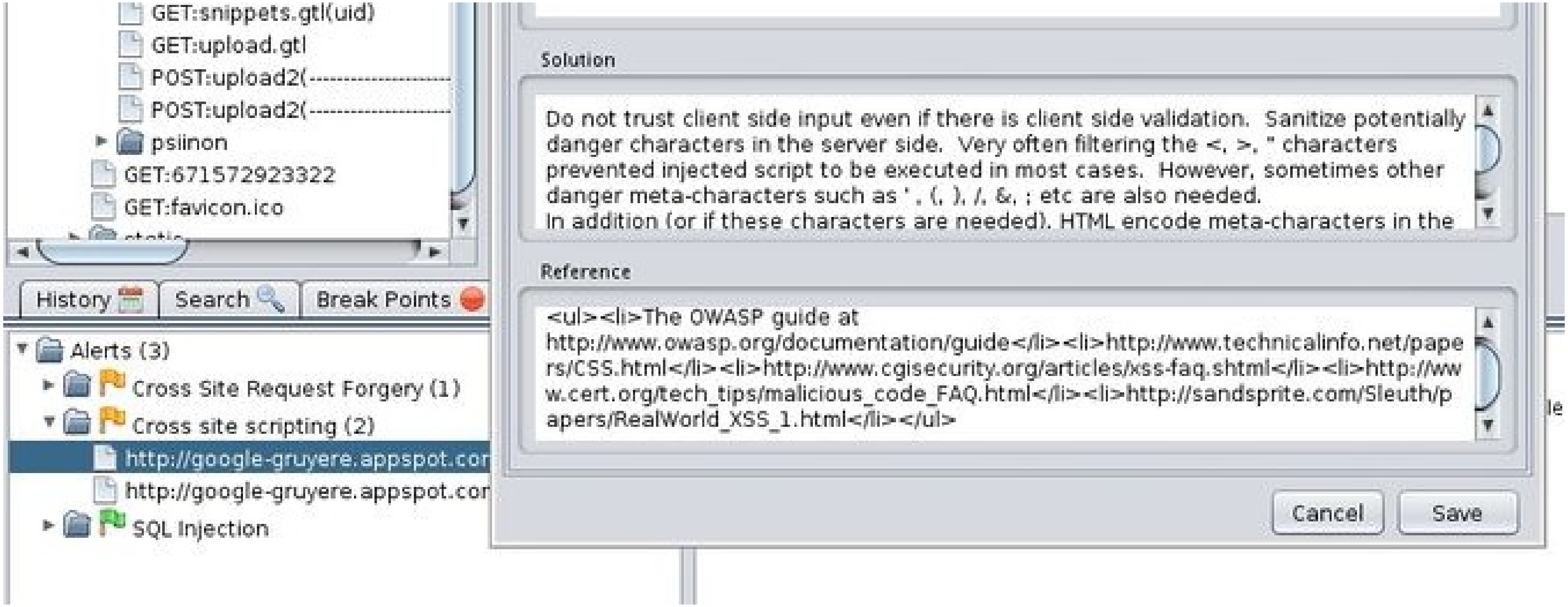
- http://192.168.x.x/mutillidae/
- you'll be able to experiment with SQL injection and many other vulnerabilities.
- Set the "hints" level to "noob" for the most helpful info :-)

Attacking with ZAP

In Kali, launch Zap from the:
Apps > Kali Linux > Top Ten > Owasp Zap

Enter the Victim IP into the Attack box: http://192.168.x.x

Run the attack, review the Alerts - includes suggested fixes !!!


GET:snippets.gtl(uid)
GET:upload.gtl
POST:upload2(--------------------
POST:upload2(--------------------
psiinon
GET:671572923322
GET:favicon.ico
History
Search
Break Points
Alerts (3)
Cross Site Request Forgery (1)
Cross site scripting (2)
http://google-gruyere.appspot.cor
http://google-gruyere.appspot.cor
SQL Injection
Cancel
Save

Solution

Do not trust client side input even if there is client side validation. Sanitize potentially danger characters in the server side. Very often filtering the <, >, " characters prevented injected script to be executed in most cases. However, sometimes other danger meta-characters such as ' , (,), /, &, ; etc are also needed.
In addition (or if these characters are needed), HTML encode meta-characters in the

Reference

<ul><li>The OWASP guide at http://www.owasp.org/documentation/guide</li><li>http://www.technicalinfo.net/papers/CSS.html</li><li>http://www.cgisecurity.org/articles/xss-faq.shtml</li><li>http://www.cert.org/tech_tips/malicious_code_FAQ.html</li><li>http://sandsprite.com/Sleuth/papers/RealWorld_XSS_1.html</li></ul>

Now you are Dangerous !!!!

- Please be careful...don't scan the internet
- It is unlawful to pentest without permission
  - get written permission, even if it is your site on some hosting company's system
- Watch YouTube vids on Metasploitable / Kali

- Feel free to contact us with your questions about cybersecurity activities at UW Bothell / OWASP:
  - Brendan Sweeney: bps7@uw.edu
  - David L. Morse: morse808@uw.edu

References

- https://www.owasp.org/images/9/9a/OWASP_Cheatsheets_Book.pdf
- https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- https://cyberarms.wordpress.com/2014/06/05/quick-and-easy-website-vulnerability-scans-with-owasp-zap/
- http://sourceforge.net/projects/metasploitable/files/Metasploitable2/
- https://www.vmware.com/support/pubs/player_pubs.html
- https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/7_0|PLAYER-710|product_downloads
- https://www.offensive-security.com/kali-linux-vmware-arm-image-download/
- http://resources.infosecinstitute.com/14-popular-web-application-vulnerability-scanners/
- https://msfbt.wordpress.com/2012/06/22/metasploitable-2-dvwa-damn-vulnerable-web-app/