Hw03 – ITEC 345: Testing web vulnerabilities.

Due: 2013.Feb.28 (Thu) 23:59.

**Notes:**

1. **Please make sure to submit the white hat agreement on D2L before working on this project. Failure to do so will mean you will get a 0 on the project.** See the hw03-dropbox-description for the agreement; sign it by typing your name and submitting back to the hw03-dropbox, *before* starting on the remainder of this assignment.
2. The lab requires you to start up a virtual machine. On a PC (windows/linux) you can download VMPlayer for free (search for VMplayer on [www.vmware.com](http://www.vmware.com) website). On Mac, download “VMPlayer Fusion”, which comes with a 30-day trial version. Contact me for a license-key good for 6mos.
3. You can use any computer in Davis Hall (they all have VMware Player installed on them), or you can install VMplayer or VMware fusion on your personal computer. You will also need to download the Owasp virtual image required for this project. (Start the 635MB download early, since it can take a while. You’ll also need enough disk space to decompress the ~2.5 GB image.). Alternatively, if you come by office hours with a thumb drive, I will load the file on it for you. Here’s how you can download the disk image:
	1. **Goto** [**http://AppSecLive.org/node/45**](http://AppSecLive.org/node/45) **website.**
	2. **Browse to the section: “Older stuff” and download: Austin Terrier VMware Install**: [**owasp-livecd-AustinTerrier-Feb2009.vmdk.rar**](http://mtesauro.com/files/owasp-livecd-AustinTerrier-Feb2009.vmdk.rar) Note: There are several images on the above website – make sure you download the Austin Terrier Feb 2009 .vmdk and not something else. This download might take a while; the file is 630MB.
	3. Un-archive/un-compress this file into a folder of your choice. Note that this is a *.rar* file. You can use stuff-it on Mac or 7-zip (<http://www.7-zip.org/>) or WinRAR on Windows to un-archive this file.
	4. Download the Owasp.vmx file from D2L🡪Dropbox🡪Hw03. Also save this to the same folder as in (c).
	5. Start up the VMPlayer. You will now see the following window, click on **Open a Virtual Machine.** 
	6. Select the file: **Owasp.vmx (browse to the folder from c)**
	7. **Select “open” at the bottom of the screen. You will see the following screen.**
	8. Select “**Play Virtual Machine**”.
	9. Ignore any warning (just say OK). **For one of the pop up windows, you will have to click on “I copied it” option.**
	10. You will be logged in. (The system may reboot sometimes, but after some time you should see a blue screen with a wasp symbol on it.
	11. **Next: the actual assignment.**

**Assignment**

*(Collaboration is allowed for this homework: feel free to discuss the homework with others, but in your submission clearly state the other students you discussed it with. Also,* ***you must finish your own homework and submit it separately****. You cannot copy or exchange screen shots.)*

**STEP 1:** Make sure you have started up the Linux virtual machine (you will see a WASP symbol). This is the OWASP live CD (the software that I left on this is from the OWASP group)**.** W**e** will now use this to run a few attacks on a web application and a database management system (MySQL - www.mysql.com).

**STEP 2:** Start up a terminal on OWASP (look for the black terminal-window icon on the bottom of the screen).

**STEP 3:** Start a program called “webgoat”, which is a buggy webserver. **On the terminal,** **simply type:**

webgoat start80

*Note: If you have previously started webgoat and are not sure if it is still running or not, simply check the status by typing:* **webgoat status**

**STEP 4:** Start up two software applications: **WebScarab** and the **Mozilla Firefox** browser.

1. **Firefox:** A transliteration of the Chinese name for a Red Panda(which is not actually a panda, but is still [danged cute](https://www.google.com/search?q=red+panda)).
2. **WebScarab:** This is the software at the bottom of the screen with a spider on its icon (next to the Firefox icon)**.** This is aweb browser *proxy* – it is used to intercept all the requests as well as data that a web client such as Firefox sends or receives. You will be using this to intercept and add malicious modifications to the web requests from the Firefox browser during the course of an attack.

**STEP 5:** Get familiar with WebScarab. Check out the various options. Specifically,

1. Change the WebScarab interface to a “Lite” interface. Search through the menu options to find this selection. The Lite interface is easier to work with. Once you select “Lite” interface close and restart WebScarab.
2. Once WebScarab restarts in Lite interface, select the “intercept” tab, check the box “intercept requests”.

**STEP 6:** in Firefox, visit the URL **http://localhost/WebGoat/attack**

**STEP 7**: Login in with the highly secure/unbreakable/inviolable/impregnable username/password: **guest/guest**

**STEP 8:** Read the warning at the bottom of the page. Commit it to memory.

**STEP 9:** Click on **Start WebGoat**.

**STEP 10:** Try to get a feel for the website. The menu bar on the left has various lessons that teach attacks. Read at least the following:

1. Introduction – How to work with WebGoat. (click on lesson plan on the top menu after selecting a topic on the right side).
2. General (which covers HTTP basics).

**STEP 11: Get familiar on how to intercept requests from the Firefox browser with WebScarab:**

1. On Firefox browser, search for the FoxyProxy plugin.
2. Once you click on this plugin, it will give you options to pick the proxy server to use.
3. **Caution:** Once you select WebScarab as your preferred proxy, remember that every web data between Firefox and any website will now be intercepted and STOPPED by WebScarab. You will have to go to the WebScarab interface and manually click on “Accept Changes” before either the data is allowed to pass to either the website or from the website to Firefox. To avoid spending too much time on this, you could only select WebScarab as the proxy when you are about to start the attack. All other times, keep FoxyProxy disabled.

**STEP 11:** Execute the following attacks. If an attack asks you to enter someone’s user name (e.g., say Tom Katz’s username and password), it will be tom/tom. When running some of these attacks, you may have to enable FoxyProxy plugin on Firefox to use WebScarab. *(Part of this exercise is self-learning – you can make use of the solution provided on the site but I strongly urge you to first see the hint, try if you can figure out how to attack, and only then see solution (if needed)).*

1. General – HTTP Splitting

Hint: follow the 'solution' steps, but be aware that (a) the virtual machine is linux (not Windows), (b) "%20" encodes a space-character (if you're curious about what they mean in the solution), and (c) you can't just paste the solution blindly; as it suggests, you have to change their example to include a date in the future.
(By the way: This attack works only because the first URL-request causes the server to respond with a 'forward to another page', which is how the input fields make it into the header, allowing the splitting.)

1. Parameter Tampering – Exploit Hidden Fields
2. Cross Site Scripting – Stage 1 Stored XSS

Hint: <script>alert("haha, made you look");</script> is valid, if poor, javascript.

1. Injection Flaws – Blind SQL injection

Hint: in SQL, strings are delimited with single-quote characters; also you can compare strings alphabetically using “>=”. So “first\_name >= 'Mjj'” will evaluate to true or false, accordingly.

***Note: After each attack is done, you will see a green check mark against the attack name. Simply take a snap shot of this to submit as your deliverable.***

**STEP 13:** Once you are done**, don’t kill the window,** instead shutdown**:** Once you are done with the security attacks or if you want to exit – click on the icon with a “K” (for KDE) on the OWASP Linux, at the lower right corner and select Log Out 🡪 Shutdown. This will ensure that your virtual machine is not damaged (not doing this but simply killing the window or closing putty SSH is like pulling the power chord to shut down a desktop or a workstation). An attack may have left the data on the disk in an unstable state and hence a shutdown is necessary.

**DELIVERABLES** Submit screen shots on D2L, one for each of the successful attacks. (In the left-hand-side menu, you will have a green check-mark next to each attack successfully completed.) When submitting, put a note in stating your team members’ names.

Extra Credit: Try and execute at least 2 additional attacks for a total of 20% extra credit. To get the credit, provide a ½ page write-up on the additional attack (attach alongside the screenshot as a .txt file – *not* .docx). The description must include: brief description of the vulnerability the attack exploits, and how it exploits it. As always, clear writing counts.