HW2

Re-submit Assignment

Due Feb 25 by 11am **Points** 100 **Submitting** a file upload **Available** after Feb 13 at 12:15pm

Web Security Project

Prerequisites

For this project, you are going to use a virtual machine running (an ancient) version of Linux. We provide basic VM images for both Oracle VirtualBox and VMware. CSL Linux machines all have VirtualBox pre-installed.

- Download Oracle's Virtual Box: https://www.virtualbox.org/wiki/Downloads (https://www.virtualbox.org/wiki/Downloads)
- Download VMware: https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/12_0 (https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/12_0)

VMware is only available free on Linux and Windows; if you have VMware fusion for Mac that may work as well.

Environment Setup

- Download the BoxesX virtual machine image (warning: 600 MB!).
- The ova file should be loaded into VirtualBox or VMware.
- Once the BoxesX VM is running, you will want to start X Window System and run the Iceweasel browser, as described below.
- The user name and password are '**user**' and '**user**'.

How to run Iceweasel

The Web server serving the Zoobar site you will be attacking is hosted inside the VM. (If you try to connect to zoobar.org outside the VM, you will get Stanford's site, which you should not try to interact with.) Furthermore, the Web browser you'll use to develop and test your attacks is also hosted inside the VM. It is called Iceweasel.

Iceweasel is the Debian version of Firefox (essentially the same browser, but with a different name because of licensing issues). To start Iceweasel in BoxesX, login as user, and do the following:

1. Type the **startx** command. This will start the X Window System, and a new window will be displayed with a xterm (shell) where you can enter commands. (Click the mouse to place the window.)
2. Type **iceweasel &** within the newly displayed xterm. This will open the Iceweasel browser. (Again, click the mouse to place the window.)
3. In the URL bar, you can type `http://zoobar.org/ (http://zoobar.org/)` to connect to the Zoobar site. As with any project, you will want to make and keep frequent backups of your work.

Project Overview

The fictional “Zoobar Foundation” has set up a simple Web application at zoobar.org (inside the BoxesX VM), allowing registered users to post profiles and transfer “zoobar” credits between each other. Each registered user starts with 10 "zoobar" credits.

You will craft a series of attacks on zoobar.org that exploit vulnerabilities in the website design. Each attack presents a distinct scenario with unique goals and constraints, although in some cases you may be able to reuse parts of your code.

Although many real-world attackers do not have the source code for the websites they are attacking, you are one of the lucky ones: you can find the source code under ***/var/zoobar/www*** in the BoxesX VM.

The Zoobar server is actually run locally on each of your boxes. We will run your attacks after wiping clean our own local database of registered users (except the user named “attacker”). Of course this means that any data you have added while working on the assignment will not be present during grading.

Before Start

Browser: We will grade your project within the BoxesX VM, using the Iceweasel browser, which is installed in the Boxes. Therefore, you should test your code in the boxes on this browser. Iceweasel is essentially the same browser as Firefox, but under different branding. Anything that works in iceweasel will likely work in (the same version of) Firefox as well. There are subtle quirks in the way HTML and JavaScript are handled by different browsers, and some attacks that work in Internet Explorer (for example) may not work in Firefox (and therefore in Iceweasel). In particular, you should use the Mozilla way of adding listeners to events (see `https://developer.mozilla.org/en/DOM/element.addEventListener (https://developer.mozilla.org/en/DOM/element.addEventListener)`).

Email script: For Attack A, you will need a server-side script to automatically email information captured by your client-side JavaScript to your user account within the Boxes. We have provided this script for you. Please review the instructions at `http://zoomail.org/sendmail.php (http://zoomail.org/sendmail.php)` (open this url from within the Boxes) and use that URL in your attack scripts to send emails. Again, this server is also being run locally on your own boxes machine. To check your local email, use the mutt email client (type ***mutt*** in the shell to start the client, and follow the instructions).

Attack A: Cookie Theft (30 pts)

- Your solution is a URL starting with `http://zoobar.org/users.php (http://zoobar.org/users.php) ?`
- The grader will already be logged into zoobar.org before loading your URL.
- Your goal is to steal the document cookie and email it to yourself using the email script.
- When sending the email with the stolen document cookie, the group name of the email has to be set to your net ID.
- Except for the browser address bar (which can be different), the grader should see a page that looks exactly as it normally does when the grader visits users.php. No changes to the site appearance or extraneous text should be visible. Avoiding the red warning text is an important part of this attack. (Its ok if the page looks weird briefly before correcting itself.)
- Hint: Here is an example attack to use as a starting point: `http://zoobar.org/users.php?user=\%22\%3E\%3Cscript\%3Ealert\%28document.cookie\%29;\%3C/script\%3E`

Attack B: Cross-Site Request Forgery (40 pts)

- Your solution is a short HTML document that the grader will open using the browser.
- The grader will already be logged into zoobar.org before loading your page.
- Transfer 10 zoobar credits from the grader's account to the "attacker" account. The browser should be redirected to `http://www.bing.com` (http://www.bing.com/) or `http://www.google.com (http://www.google.com)` as soon as the transfer is complete (so fast the user might not notice).
- The location bar of the browser should not contain `zoobar.org` at any point.

Attack C: SQL Injection (30 pts)

- Your solution is a short HTML document that the grader will open using the browser.
- The grader will not be logged into zoobar.org before loading your page.
- Your HTML document should display a form with a text field and a button. The grader will type a username into the text field and press the button.
- As a result, the grader should be logged into zoobar.org as the user whose name was typed in the text field. The browser's location bar should be redirected to `http://zoobar.org/index.php (http://zoobar.org/index.php)`, and the page should look and behave exactly as if the grader had instead typed the username and corresponding password in the legitimate zoobar.org login form.
- The name the grader types in will already be registered with some password. You do not need to handle the case in which the name was not already registered.
- Hint: What part of the zoobar.org PHP code handles the user login and registration, and how does it interface with the SQLite database?

Tips

- If you need to transfer files from your main machine to your virtual machine, there is a command to use: scp -r -P 8024 <your file(s)> user@127.0.0.1:<target path in your vm> .
- The zoobar source files are here: **HW2-zoobar.zip** **HW2-zoomail.zip**

Collaboration Policy

This assignment is to be done individually. You are encouraged to use the internet or talk to classmates for information about tools and setup. Please help your fellow classmates with setup and understanding HTML , JavaScript or SQL, but don't discuss solution specifics with anyone. Remember, searching for homework solutions online is **academic misconduct**. If two students' submissions are very similar --- for some definition of similarity --- both students will get zero points for this assignment.

Deliverables

- You should include a `README.txt` file , describing the vulnerabilities and your attacks; and the other 3 files `a.txt, b.html, c.html` corresponding to 3 attacks respectively.
- Put all 4 files in a directory named your net ID (i.e., prefix of your wisc email) and compress it to a zip.

Grading

If the attack works, one will receive full credit. Partial credit will be given for a good description of the vulnerability and how an exploit should work.

HW2 Rubric

Criteria	Ratings	Pts
Attack A Explanation		10.0 pts
Successful Implementation		20.0 pts
Attack B Explanation		10.0 pts
Successful Implementation		30.0 pts
Attack C Explanation		10.0 pts
Successful Implementation		20.0 pts
		Total Points: 100.0