Intro To Info Security: Project #4.5

Due on August 1st, 2016

Professor Wenke Lee

Web Security-Optional

Contents

Setting Up

Please download the VM from : `https://www.prism.gatech.edu/~gwang312/websec2.ova`
You should be able to open the file and set up a VM directly with VirtualBox.
The logins (username/password) are as follows:

root/root

user/user

You are required to use *root/root* to complete the project, but feel free to explore using root.
Our support will be VirtualBox on major OS (Ubuntu, Windows, OSX).

Interacting with the VM

Option 1: Port forwarding and ssh
Xorg and openssh-server are set up on the VM, so you may set up port forwarding from VirtualBox. This can be done by:

Right click on VM → Settings → Network → Advanced → Port Forwarding.

Enter: name:ssh, protocol:TCP, hostport:2222 (or anything you prefer), guestport:22. Leave others blank.

You may then ssh in with

ssh -p 2222 -Y user@127.0.0.1

Other use include *sshfs* and *scp*, which you may explore yourself.

Option 2: Old fashion login.
After logging in, you should be able to start up a desktop with **startx** command. This will prompt up a minimal LXDE desktop environment that is sufficient for you to complete the project. If you wish to install more packages, you may do so with apt-get. To change resolution, you may use the **xrandr** command.

Georgia Tech Payroll

The site we will be exploiting in this project is **payroll.gatech.edu**. Please note that this is a made-up site and does not point to a legit site in the real world. For testing purposes, you may register accounts at your will. However, **please DO NOT use your actual passwords and banking information.**

The source code of the site can be found in **/var/payroll/www**. We will be using iceweasel, which is provided in the VM, to test your exploits. You may also assume JavaScript is always enabled in iceweasel.

Disclaimer

This project is solely for educational purposes.
Wenke Lee or any affiliation associated with him or his research/teaching is NOT responsible in the event of any criminal charges be brought against any individuals misusing the information in this project to break the law.
When in doubt, please consult the TAs or Professor Lee regarding any issues.

Task 1: XSRF Prevention (40 points)

It's my first day working on the Gatech payroll site. This site needs some serious rework; it looks so 90s. Perhaps I can start off by making the site look more appealing... wait, this doesn't look right. As I pulled up the database for our service, it looks like a lot of the accounts are pointing to the same account and routing number. It looked rather suspicious, so I contacted Gatech InfoSec. Meanwhile, I started looking into our code base. "Aha, I see. I guess I'll have to fix this vulnerability now."

Deliverable: Please patch up the vulnerability mentioned in Project 4 Target #1 and (1) provide a write up in report.pdf about how you patched it up and contents of your patched code.(2) Why it is secure now. (3)Also explain why Same Origin Policy cannot prevent such an attack.

Task 2: XSS Prevention (20 points)

Ah so it was a kid that was responsible for this attack. He's quite smart actually, so I guess that's why InfoSec decided to recruit him for pen testing. He was able to show me another XSS attack to the website, so I'll have to fix that as well. Though I feel like this kid is still up to no good. Perhaps I should keep an eye on him.

Deliverable: Please patch up the vulnerability mentioned in Project 4 Target #2 and (1) provide a write up in report.pdf about how you patched it up and contents of your patched code. (2) why it is secure now. (3) Also explain why Same Origin Policy cannot prevent such an attack.

Task 3: SQL Injection Prevention (20 points)

I decided to check the login activities dashboard one last time before I leave work today. I saw quite a few logins for various account came from the kid. Seems like he's testing some things. I'm sure he'll let me know what's going on tomorrow morning.
"Oh ***." Our systems just caught that a large amount of logins were happening on the same external IP when I was about to go to bed. Was it that kid? I tried to contact the kid to see what he's up to but to no avail. I can't wait any longer, and have find and fix it ASAP. My gut says it may be a SQL injection attack. Let me see if I can patch it up.

Deliverable: Please patch up the vulnerability mentioned in Project 4 Target #3, and (1)provide a write up in report.pdf about how you patched it up and the contents of your patched code. (2) why is it secure now.

Task 4: Further Security Fortification (20 points)

Thank goodness it was the law enforcement at work. I can't imagine if it was an actual hacker group access to our service. I guess this kid got what he deserved. I know this won't be a one time thing, so I wonder if there are other vulnerabilities?

Deliverable: Are there any other vulnerabilities? (1) Please document them in report.pdf and patch them up if applicable. Also include how you found them. (2) Please put the contents of your patched code in the pdf. (3) If there are more vulnerabilities, but is out of your control to fix it, also document them and describe why it can't be fixed.

Deliverables and Requirements

- report.pdf: containing your gt id, eg. jdoe3. Unlike project#4, report.pdf will be a major part of your grade, so please write them up neatly and concisely. Please also justify clearly; Any ambiguity may result in deductions (This may be graded more strictly as it counts as extra credit).
- payroll.zip: the code you patched up in /var/payroll. The folder structure should be preserved; ie. simply zip up /var/payroll into payroll.zip without flattening the structure. (You may need to install zip in the VM.) Please also note that the user experience should be the same after your fixes. For example, if a code is broken, you can't simply remove it and claim that it is fixed.

Tips/Hints

- After changing the code in /var/payroll/www, type

  service apache2 restart

  as root to reload the site with your changes.
- XSRF paper: http://seclab.stanford.edu/websec/csrf/csrf.pdf

Acknowledgement

Special thanks to Professor V. Shmatikov for the inspiration of this project and his permission to modify/reuse his materials. You may find more about him and his research at: `http://www.cs.cornell.edu/~shmat/`