Intro To Info Security: Project #4

Due on August 4th, 2016

Professor Wenke Lee

Web Security

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 should only use *user/user* to complete the project. root/root credentials are provided for your convenience in case you need to install extra software/packages.

Interacting with the VM

Option 1: Port forwarding and ssh (Instructions presumes you have Unix/Linux systems)
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 -X 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 with root. 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.

There are 3 targets in total (100 points). **Please check Deliverables section for what to submit.** Good luck and have fun.

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.

Target 1: XSRF (30 points)

You stumbled upon the GaTech payroll website and found a vulnerability. Suppose a user (let us say, Alice) is already logged in the GaTech payroll site. You noticed that you can craft a webpage so that when Alice visits your webpage, she gets redirected (**NO popups**) to the GaTech payroll page with her account number and routing number set to some values of your choice.
Poor and living off on ramen, you decide to give it a try and craft the web page to set the banking information to yours:

account number: **2133721337**

routing number : **4242424242**

The user must not see the contents of your crafted page (a split second due to browser rendering is acceptable)!

Deliverable: t1.html, [optional] report.pdf. Not following naming format results in an automatic failure (0 points).

Sample deliverable: t1.html

```
<body onload="document.forms[0].submit()">
<form action="" onsubmit="" method="POST">
<!-- your exploits here
you may also want to change some form attributes-->
</form>
</body>
```

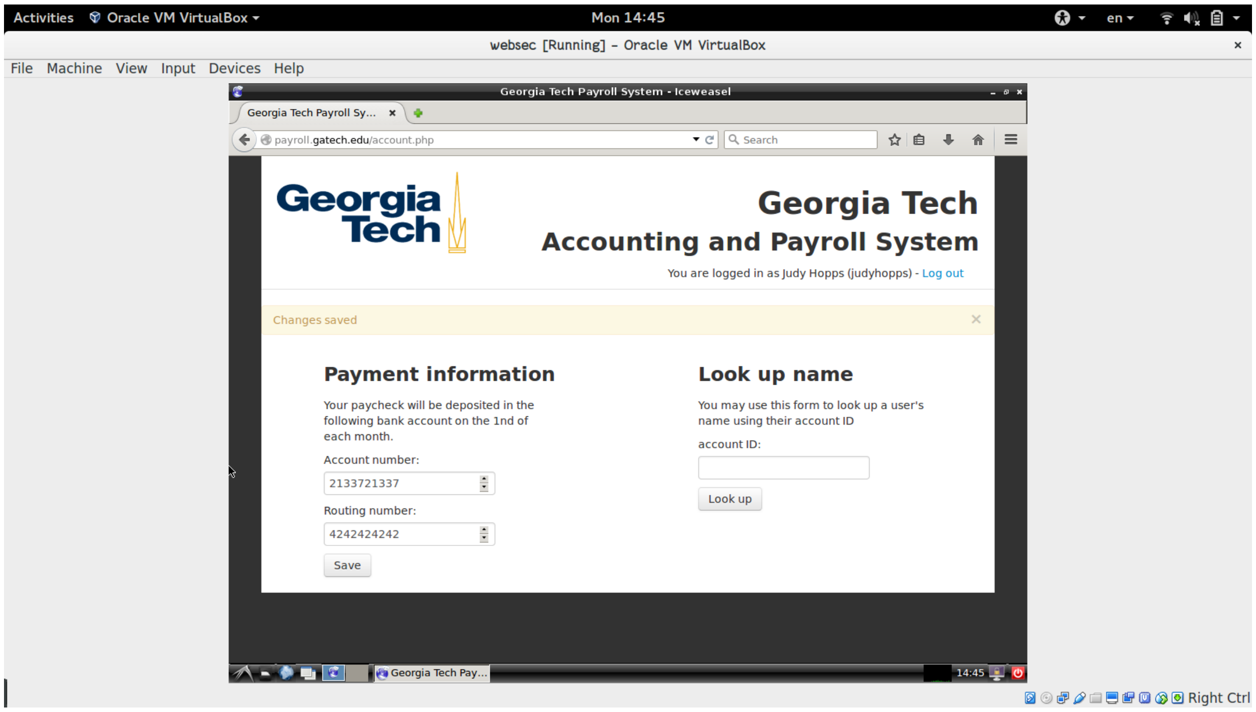
report.pdf

```
Target <?>
The vulnerable code is in <filename>:<line>
because <reason>
<Provide screenshot if applicable>
```

Milestones
A successful attack gains 30 points automatically.
If you are unable to complete the task, you will be paid accordingly by the milestones as follows:

- 10 points: Identify vulnerability and briefly explain why it is vulnerable. Provide it in report.pdf.
- 10 points: if you are able to see "XSRF prevented" message with you exploit.
- 10 points: Able to change the account and routing info without extra tabs or popups.

Note: You can visit your webpage by typing the path of your file in the url bar, eg. `file:///home/user/t1.html` given that your exploit lives in */home/user/*.


Activities
Oracle VM VirtualBox
Mon 14:45
websec [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Georgia Tech Payroll System - Iceweasel
payroll.gatech.edu/account.php
Right Ctrl

Georgia Tech
Accounting and Payroll System

You are logged in as Judy Hopps (judyhopps) - Log out

Changes saved

Payment information

Your paycheck will be deposited in the following bank account on the 1nd of each month.

Account number: 2133721337

Routing number: 4242424242

Save

Look up name

You may use this form to look up a user's name using their account ID

account ID:

Look up

Example of Successful exploit

Target 2: XSS-password theft (40 points)

You were caught! Good thing is Gatech InfoSec was curious if you can find anything else more severe, and would let you off the hook if you help them out. You noticed that you are able to steal passwords; you can craft a webpage such that whenever a victim (let's say, Bob) visits the page, it will redirect (no popups) him to http://payroll.gatech.edu/. The webpage should look as if Bob visited the site directly. When Bob types in his user/password and hits login, an email containing the credentials will be sent. GaTech administrators would like you to demonstrate the attack and pay you accordingly. You will have to send the mail to *user* as a proof of concept.

This attack will require an email to be sent to **user** on the system. Good thing is you can use hackmail: `http://hackmail.org/sendmail.php` (open this URL from within the vm for more instructions) to send emails via your attack scripts. Any mail the user receives will appear in /var/mail/user.

Requirements:

- This attack must be done via XSS; providing a phishing webpage will result in 0 points, ie. the url bar should contain the domain "payroll.gatech.edu" and not a phishing url.
- The format of the email payload should be "<username> <password>." ie. victim's username followed by a space and then the victim's password. You may assume that the username and password does not contain whitespaces. The sender should be set to "haxor".
- Redirected page must be cosmetically identical to the original page. The webpage source can be different as long as the user can't notice without looking at the source.

Deliverable: t2.html,[optional] report.pdf. Not following naming format results in an automatic failure (0 points).

Sample deliverable: t2.html

```
<body onload="document.forms[0].submit()">
<form action="" onsubmit="" method="POST">
<!-- your exploits here
you may also want to change some form attributes-->
</form>
</body>
```

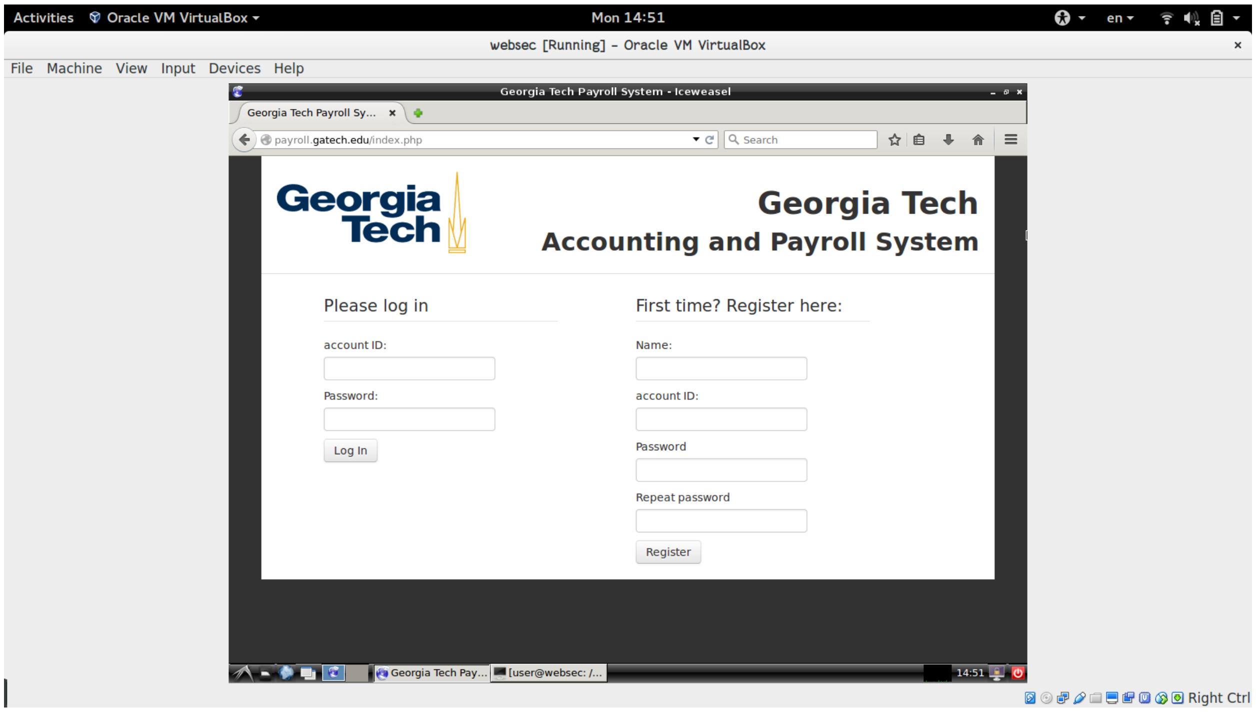
report.pdf

```
Target <?>
The vulnerable code is in <filename>:<line>
because <reason>
<Provide screenshot if applicable>
```

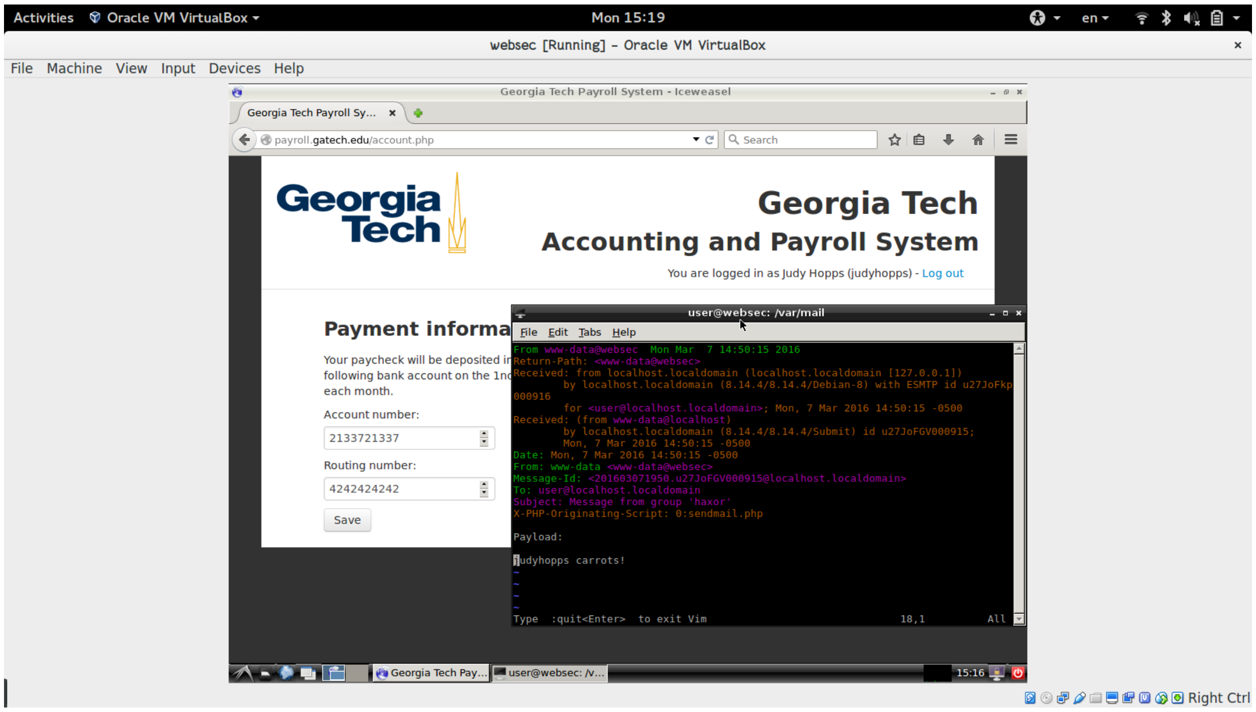
Milestones
A successful attack gains 40 points automatically.
If you are unable to complete the task, you will be paid accordingly by the milestones as follows:

- 10 points: Identify vulnerability and briefly explain why it is vulnerable. Provide it in report.pdf.
- 20 points: Able to steal the username/password and send it via the mail.
- 10 points: the exploited webpage is cosmetically the same as original site.

Example of Successful exploit


Activities
Oracle VM VirtualBox
Mon 14:51
websec [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Georgia Tech Payroll System - Iceweasel
Georgia Tech Payroll Sy...
payroll.gatech.edu/index.php
Search
Georgia Tech
Georgia Tech
Accounting and Payroll System
Please log in
account ID:
Password:
Log In
First time? Register here:
Name:
account ID:
Password
Repeat password
Register
Georgia Tech Pay...
[user@websec: /...
14:51
Right Ctrl

After visiting h2.html, it should look exactly the same as the legitimate site.


Activities
Oracle VM VirtualBox
Mon 15:19
websec [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Georgia Tech Payroll System - Iceweasel
Georgia Tech Payroll Sy...
payroll.gatech.edu/account.php
Search
Georgia Tech
Georgia Tech
Accounting and Payroll System
Log out
Payment informa
Save
user@websec: /var/mail
File Edit Tabs Help
Georgia Tech Pay...
user@websec: /v...
15:16
Right Ctrl

You are logged in as Judy Hopps (judyhopps) - Log out

Your paycheck will be deposited i
following bank account on the 1n
each month.

Account number: 2133721337

Routing number: 4242424242

```
From www-data@websec  Mon Mar  7 14:50:15 2016
Return-Path: <www-data@websec>
Received: from localhost.localdomain (localhost.localdomain [127.0.0.1])
        by localhost.localdomain (8.14.4/8.14.4/Debian-8) with ESMTP id u27JoFkp
000916
        for <user@localhost.localdomain>; Mon, 7 Mar 2016 14:50:15 -0500
Received: (from www-data@localhost)
        by localhost.localdomain (8.14.4/8.14.4/Submit) id u27JoFGV000915;
        Mon, 7 Mar 2016 14:50:15 -0500
Date: Mon, 7 Mar 2016 14:50:15 -0500
From: www-data <www-data@websec>
Message-Id: <201603071950.u27JoFGV000915@localhost.localdomain>
To: user@localhost.localdomain
Subject: Message from group 'haxor'
X-PHP-Originating-Script: 0:sendmail.php

Payload:

judyhopps carrots!
~
~
~
~
Type  :quit<Enter>  to exit Vim                              18,1          All
```

After user types in credentials, it should log in successfully, and an email should be sent.

Target 3: SQL Injection (30 points)

H4x0r0rg has heard about your feat in making tons of money from GaTech by changing other people's payroll account. They contacted you and gave you a job, a job with a hefty sum you can't resist. The task is to create an html webpage, and the requirements are the following:

- They want you to craft a page with a text field for username and a submit button. (**NO password field!**)
- The user of this page is not logged into GaTech payroll system, but when they enter a valid GaTech payroll registered username (suppose it's judyhopps) and hit submit, the user will be redirected to **payroll.gatech.edu/account.php** logged in as judyhopps.
- Do NOT execute destructive SQL commands eg. DROP tables. System admins can easily detect data loss!
- The id of the input field must be "targetlogin", and the button id must be "exploit". For example:
  <input name="login" id="targetlogin" value="username">
  <button id="exploit">Hold on to your butts!</button>

Deliverable: t3.html,[optional] **report.pdf** Not following naming format results in an automatic failure (0 points).

Sample deliverable: t3.html

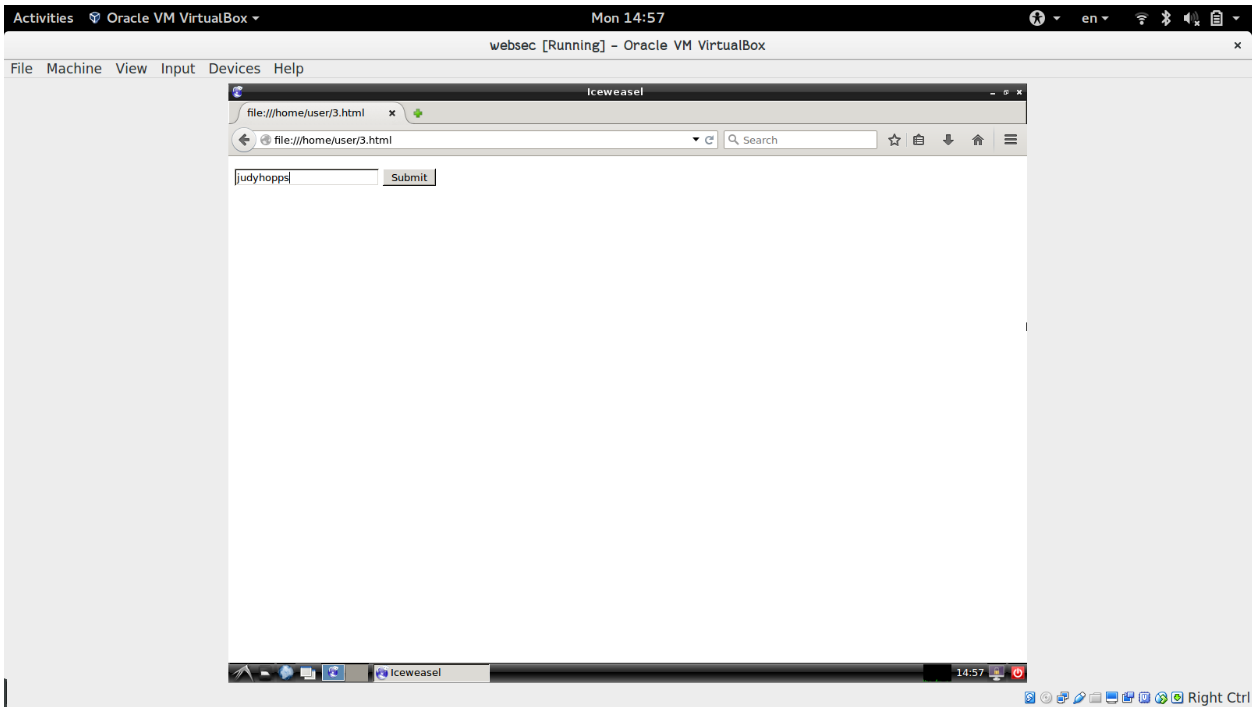
```
<body>
<form action="" onsubmit="" method="POST">
<!-- same drill. forms in this format if you need it-->
</form>
<input name="login" id="targetlogin" value="username">
<button  id="exploit" onclick="">Hold on To Your Butts!</button>

<script type="text/javascript">
<!-- some script here if you need it -->
</script>
</body>
```

report.pdf

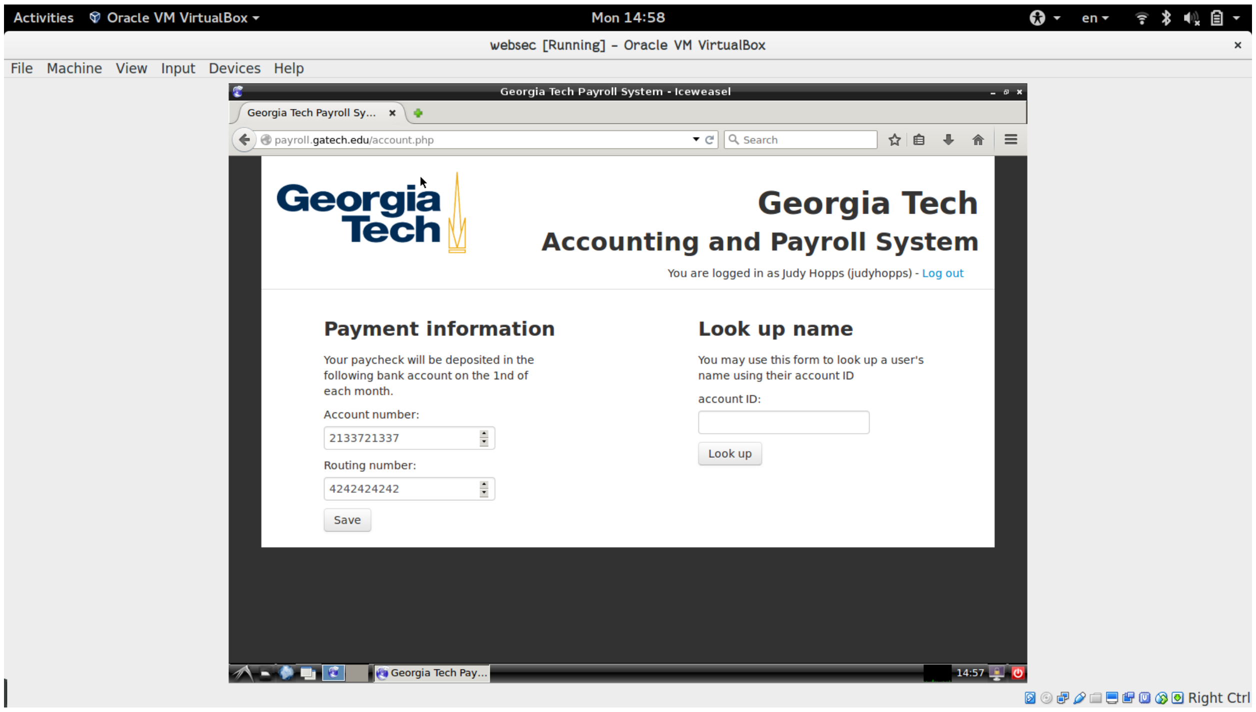
```
Target <?>
The vulnerable code is in <filename>:<line>
because <reason>
<Provide screenshot if applicable>
```

Milestones
A successful attack gains 30 points automatically.
If you are unable to complete the task, you will be paid accordingly by the milestones as follows:

- 10 points: Identify vulnerability and briefly explain why it is vulnerable. Provide it in report.pdf.
- 20 points: Actual webpage impl.
- If you implemented the attack with a destructive SQL command and causes our scripts to fail to grade your other targets, you will not be getting any partial credits for those failed targets.



After visiting h3.html, it should contain an input field for the attacker. Feel free to prettify it as long as it complies with the requirements.


Activities
Oracle VM VirtualBox
Mon 14:58
websec [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Georgia Tech Payroll System - Iceweasel
payroll.gatech.edu/account.php
Georgia Tech
Accounting and Payroll System
You are logged in as Judy Hopps (judyhopps) - Log out
Payment information
Your paycheck will be deposited in the following bank account on the 1nd of each month.
Account number:
2133721337
Routing number:
4242424242
Save
Look up name
You may use this form to look up a user's name using their account ID
account ID:
Look up
Right Ctrl

After user types in the username, it should log in successfully. The site should function as if logged in legitimately.

Epilogue

You delivered your exploit to H4x0r0rg. They seemed quite happy, and so are you. Just the thought of not having to work for the rest of your life seems quite enticing. But then you heard the FBIs knocking on your door. Turns out H4x0r0rg was just a bait from the law enforcers!

Deliverable: Please do not do this in the real world.

Deliverables Summary/Requirements

Please submit them as separate files. Do **NOT** zip them.
Not following this rule will result in a **50%** penalty.

- [**Required**] t1.html, t2.html, t3.html
- [**Optional**] report.pdf, please include your gtid, eg. jdoe3. Report.pdf is not necessary, but it's to your benefit to have it for partial credit in case your exploits didn't work.

Helpful Readings/ Hints

- This assignments requires form submission. If you do not know how to do so, you may consult `http://www.w3schools.com/html/html_forms.asp`.
- This assignment (especially for target 3) may require some javascripting. Only a very basic knowledge is needed. You may find `http://eloquentjavascript.net/` useful if you're completely new to javascript.
- You do not need to know extensive SQL knowledge to complete target 3, however, it requires a little more observation and thinking.
- The sample deliverables are there for your benefit/convenience. You are not required to follow the format. As long as the exploit works according to requirements, you will receive full credit.

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/`