

Intro To Info Security: Project #4

Due on 7 December 2016 at 12:00AM EST

Professor Wenke Lee

Web Security

Contents

Setting Up	3
Interacting with the VM	3
Georgia Tech Payroll	3
Deliverables Summary/Requirements	3
Disclaimer	4
Target 1: XSRF (20 points)	5
Target 2: XSS-password theft (30 points)	7
Target 3: SQL Injection (20 points)	9
Epilogue (30 points)	11
Helpful Readings/ Hints	11
Acknowledgement	11

Setting Up

The virtual appliance for this project is available via the following venues:

- Web: <http://evan.gtisc.gatech.edu/cs6035/project4/OMS-CS6035-Project4-WebSec.ova>
- Torrent: <magnet:?xt=urn:btih:134a94b7f7237091d787ce3613fa354dfc3c6be7&dn=OMS-CS6035-Project4-WebSec.ova>. A .torrent file is also provided as an attachment in the project's T-Square.

You are provided both root and regular user access to this appliance with the following credentials:

- 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

Xorg and openssh-server are set up on the VM, and the virtual appliance is preconfigured to forward the host's port 2222 to the appliance's port 22. So you can ssh in with

```
ssh -p 2222 -X user@127.0.0.1
```

You can also launch the appliance in GUI mode. After logging in, you can start a minimal LXDE environment with the command `startx`. Virtualbox guest additions have been preinstalled on the VM. If you wish to install more packages, you may do so with `apt-get` as root.

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 Firefox, which is provided in the VM, to test your exploits. You may also assume javascript is always enabled in Firefox.

There are 3 targets in total worth 70 points, and a brief writeup worth an additional 30 points. **Please check Deliverables section for what to submit**. Good luck and have fun.

Deliverables Summary/Requirements

Please submit them as separate files. Do **NOT** zip them.

Not following this rule will result in a **50%** penalty.

- t1.html, t2.html, t3.html
- report.pdf, please include your gtid, eg. jdoe3. This should contain the required responses to the Epilogue section, as well as any of the partial credit responses you wish to include for each target.

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 (20 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>
```

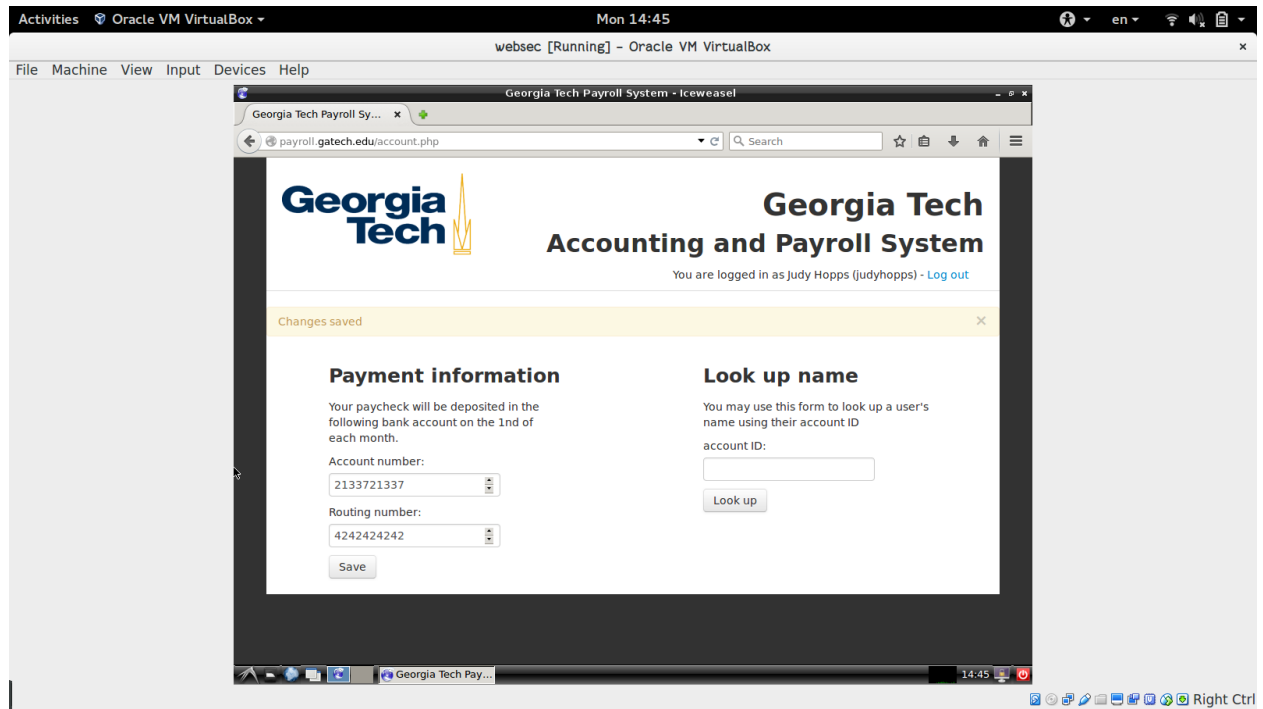
Milestones

A successful attack gains 20 points automatically.

If you are unable to complete the task, you will be paid accordingly by the milestones as follows:

- 6 points: Identify vulnerability and briefly explain why it is vulnerable. Provide it in report.pdf.
- 7 points: if you are able to see "XSRF prevented" message with you exploit.
- 7 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/.



Example of Successful exploit

Target 2: XSS-password theft (30 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 30 points automatically.

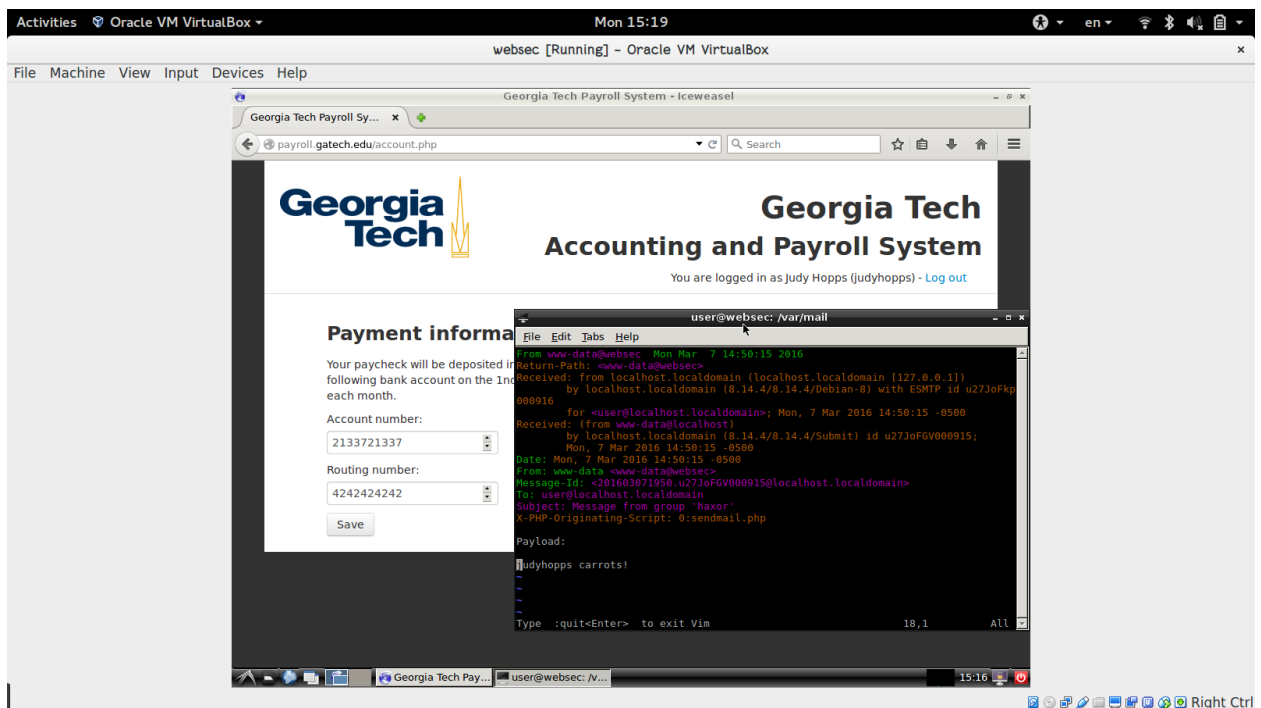
If you are unable to complete the task, you will be paid accordingly by the milestones as follows:

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

Example of Successful exploit



After visiting t2.html, it should look exactly the same as the legitimate site.



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

Target 3: SQL Injection (20 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>
5 <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 -->
10 </script>
</body>
```

report.pdf

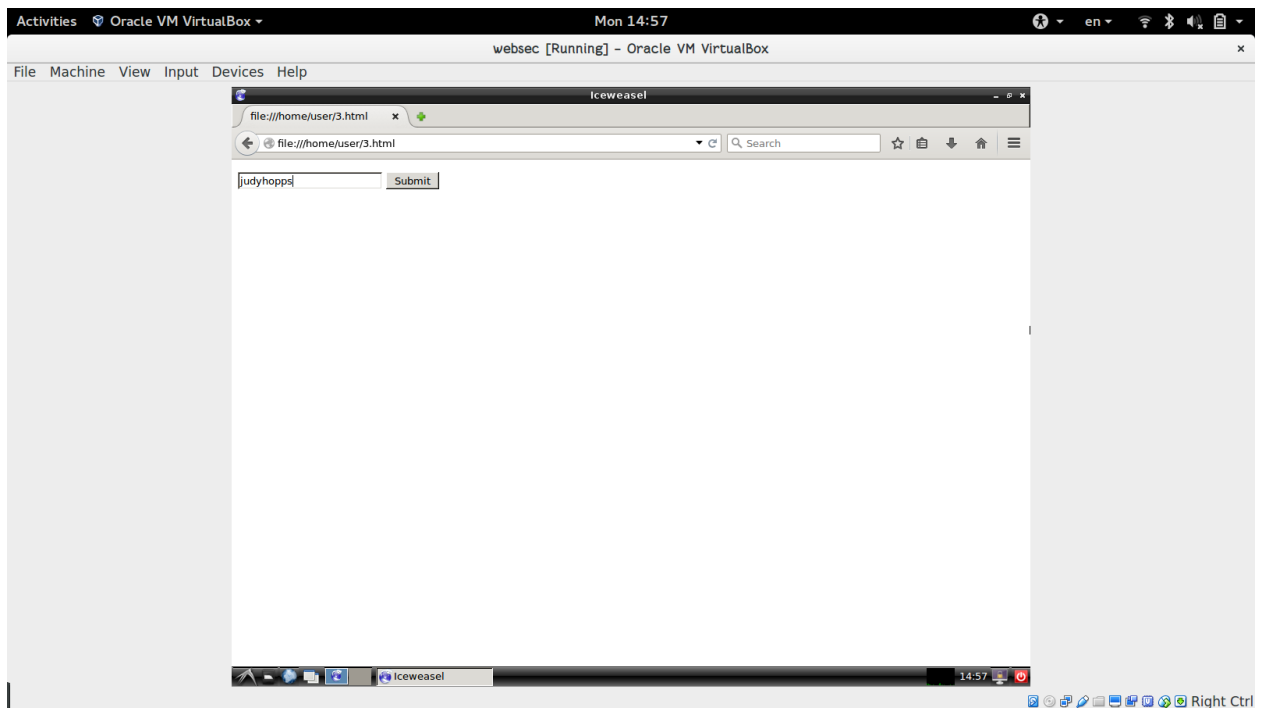
```
Target <?>
The vulnerable code is in <filename>:<line>
because <reason>
<Provide screenshot if applicable>
```

Milestones

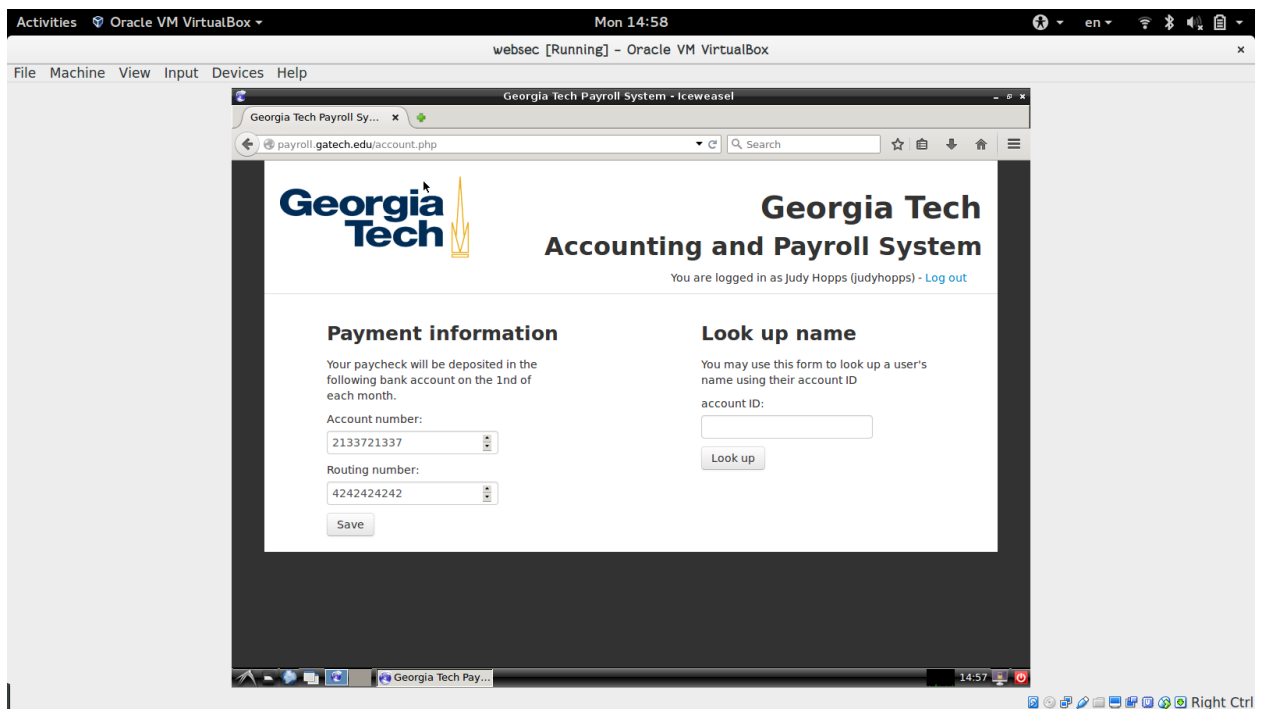
A successful attack gains 20 points automatically.

If you are unable to complete the task, you will be paid accordingly by the milestones as follows:

- 5 points: Identify vulnerability and briefly explain why it is vulnerable. Provide it in report.pdf.
- 15 points: Actual webpage implementation.
- 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 credit for those failed targets.



After visiting t3.html, it should contain an input field for the attacker. Feel free to prettify it as long as it complies with the requirements.



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

Epilogue (30 points)

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 FBI knocking on your door. Turns out H4x0r0rg was just a law enforcement honeypot!

They're willing to let you off the hook – this time – but only if you do some work in restitution first.

For each of the three targets, describe briefly in `report.pdf` how to fix the vulnerabilities you found so that they can no longer be exploited. You do *not* need to include actual patched code; however, your descriptions should be sufficiently detailed that they would be actionable.

Deliverable: `report.pdf`

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/>