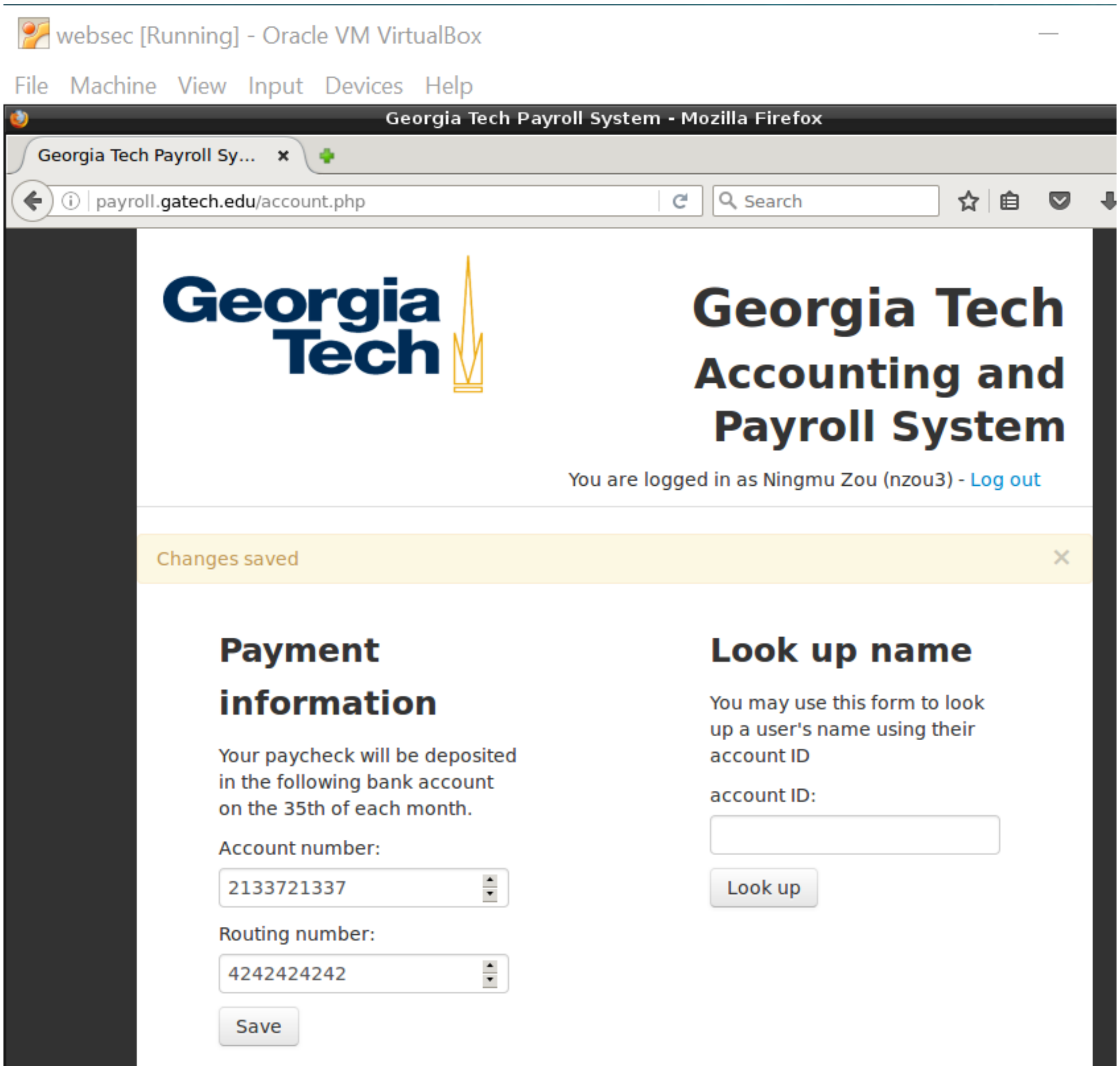
CS6035 2016 Fall
Ningmu Zou
nzou3@gatech.edu
Target <1>

the vulnerable code is in account.php.

Because input fields are included in a POST request to that page and there is a hashcode function generated. Attackers can set the banking information to any number by matching the hashcode.

In order to get avoid of this vulnerability, POST response should be modified so that no attacker can guess the possible value with hidden type.


websec [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Georgia Tech Payroll System - Mozilla Firefox
Georgia Tech Payroll Sy...
payroll.gatech.edu/account.php
Search
Georgia Tech

Georgia Tech Accounting and Payroll System

You are logged in as Ningmu Zou (nzou3) - Log out

Changes saved

Payment information

Your paycheck will be deposited in the following bank account on the 35th 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:

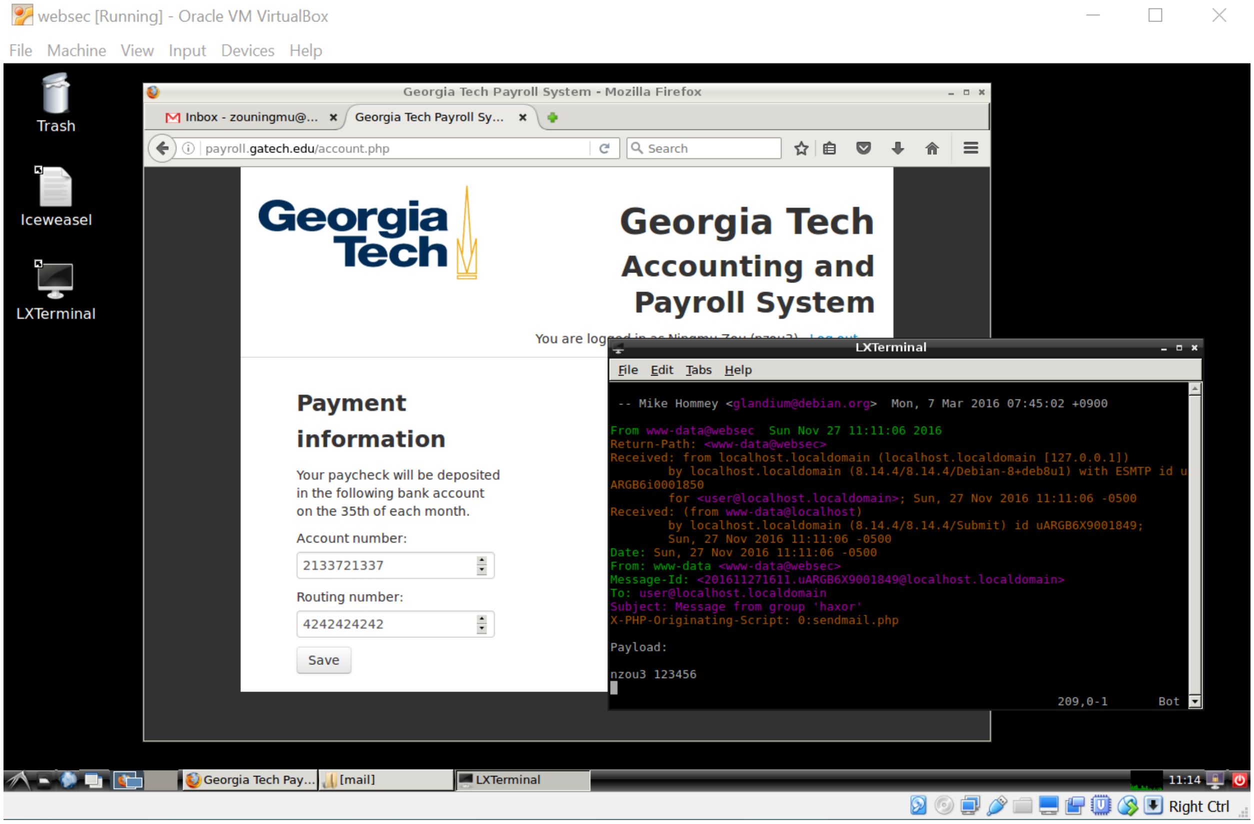
Look up

CS6035 2016 Fall
Ningmu Zou
nzou3@gatech.edu
Target <2>

The vulnerable code is in index.php

The reason is there is no input validation in login input value field when a user tries to log in the system with username and password. This vulnerability leaves a chance for attackers to insert or apply some malicious javascript into the website. Attackers only need to execute a function which can record and steal the username and password and email the personal information.

In order to get avoid this vulnerability, a login input value validation should be added so that no one can bypass and add any arbitrary javascript into the website. With this authentication method, the login personal information could become safer through the website.


websec [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
Iceweasel
LXTerminal
Georgia Tech Payroll System - Mozilla Firefox
Inbox - zouningmu@...
Georgia Tech Payroll Sy...
payroll.gatech.edu/account.php
Search
Georgia Tech
LXTerminal
File Edit Tabs Help
Georgia Tech Pay...
[mail]
LXTerminal
11:14
Right Ctrl

Georgia Tech Accounting and Payroll System

You are logged in as Ningmu Zou (nzou3). Log out

Payment information

Your paycheck will be deposited in the following bank account on the 35th of each month.

Account number: 2133721337

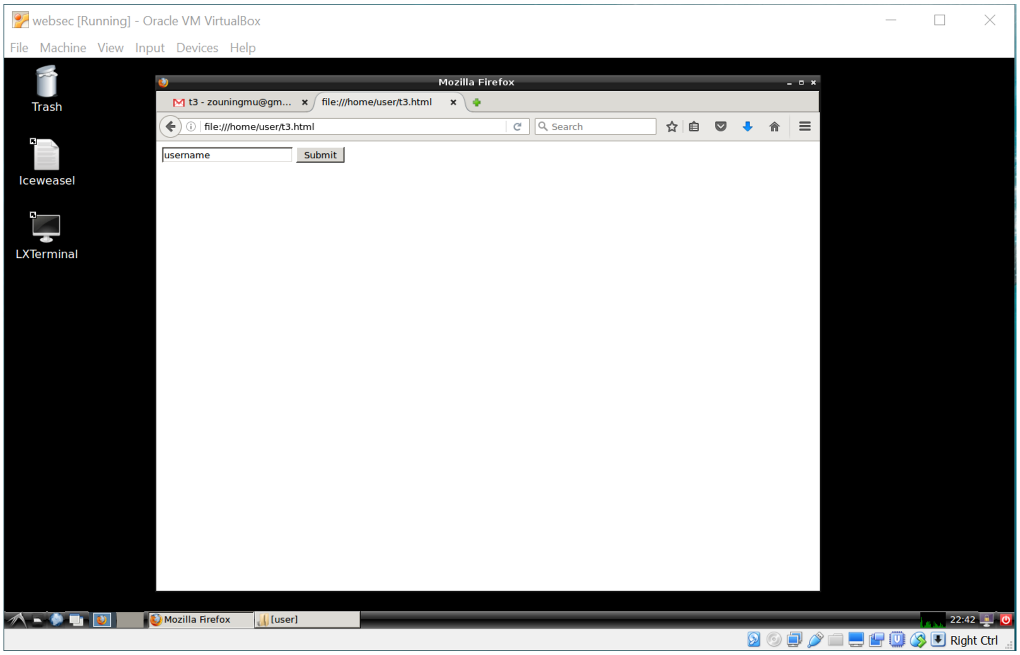
Routing number: 4242424242

Save

```
 -- Mike Hommey <glandium@debian.org>  Mon, 7 Mar 2016 07:45:02 +0900

From www-data@websec  Sun Nov 27 11:11:06 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+deb8u1) with ESMTP id u
ARGB6i0001850
        for <user@localhost.localdomain>; Sun, 27 Nov 2016 11:11:06 -0500
Received: (from www-data@localhost)
        by localhost.localdomain (8.14.4/8.14.4/Submit) id uARGB6X9001849;
        Sun, 27 Nov 2016 11:11:06 -0500
Date: Sun, 27 Nov 2016 11:11:06 -0500
From: www-data <www-data@websec>
Message-Id: <201611271611.uARGB6X9001849@localhost.localdomain>
To: user@localhost.localdomain
Subject: Message from group 'haxor'
X-PHP-Originating-Script: 0:sendmail.php

Payload:

nzou3 123456

                                                           209,0-1       Bot
```

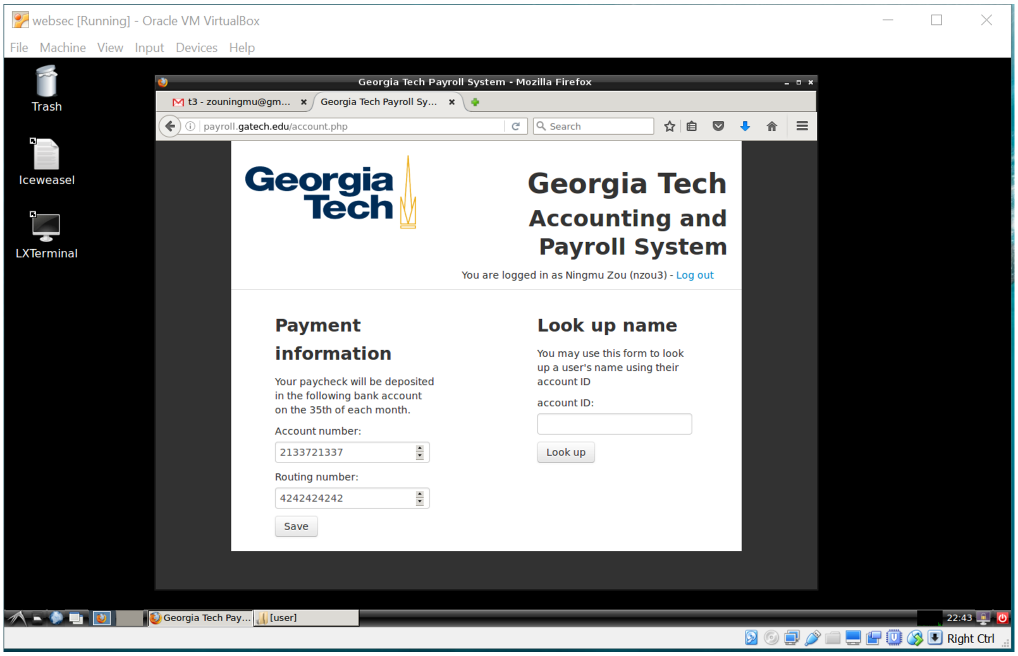
CS6035 2016 Fall
Ningmu Zou
nzou3@gatech.edu
Target <3>

The vulnerable code is in index.html because single quotes with double quotes is allowed in the code and this would allow a SQL injection with arbitrary SQL statement. In order to get avoid of this vulnerability, an input verification should be added into the code and such as “’” should never be allowed in the SQL statement so a registered user would only use his/her own login username and password to login the system without interfering any other users.



file:///home/user/t3.html

username [Submit]


websec [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
Iceweasel
LXTerminal
Georgia Tech Payroll System - Mozilla Firefox
t3 - zouningmu@gm...
Georgia Tech Payroll Sy...
Search
Georgia Tech
Georgia Tech Pay...
[user]
22:43
Right Ctrl

payroll.gatech.edu/account.php

Georgia Tech Accounting and Payroll System

You are logged in as Ningmu Zou (nzou3) - Log out

Payment information

Your paycheck will be deposited in the following bank account on the 35th 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]