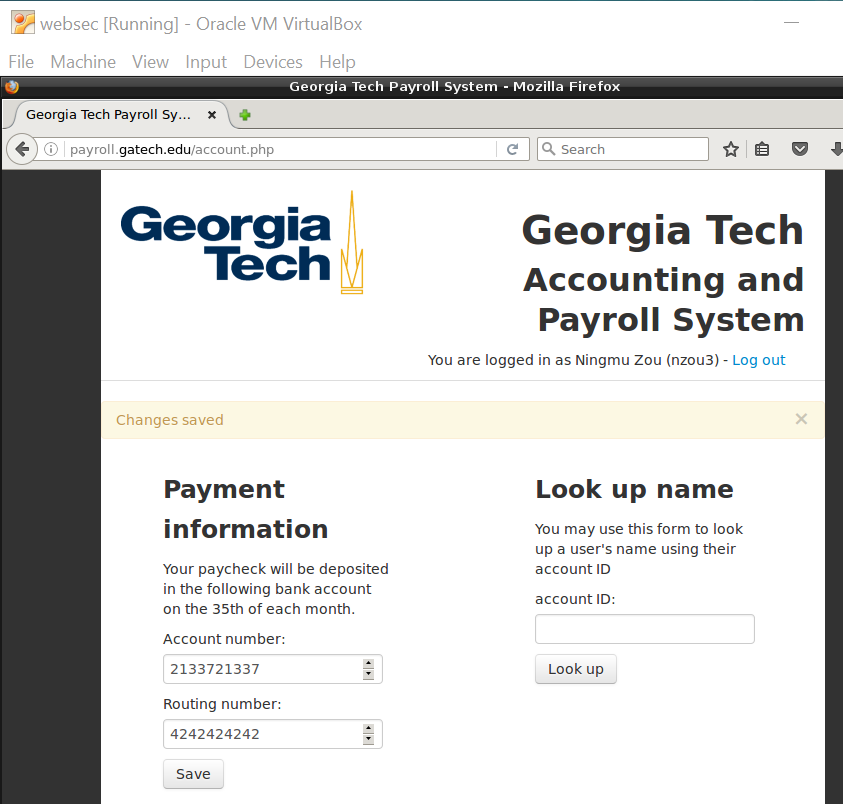
Target <1>

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.

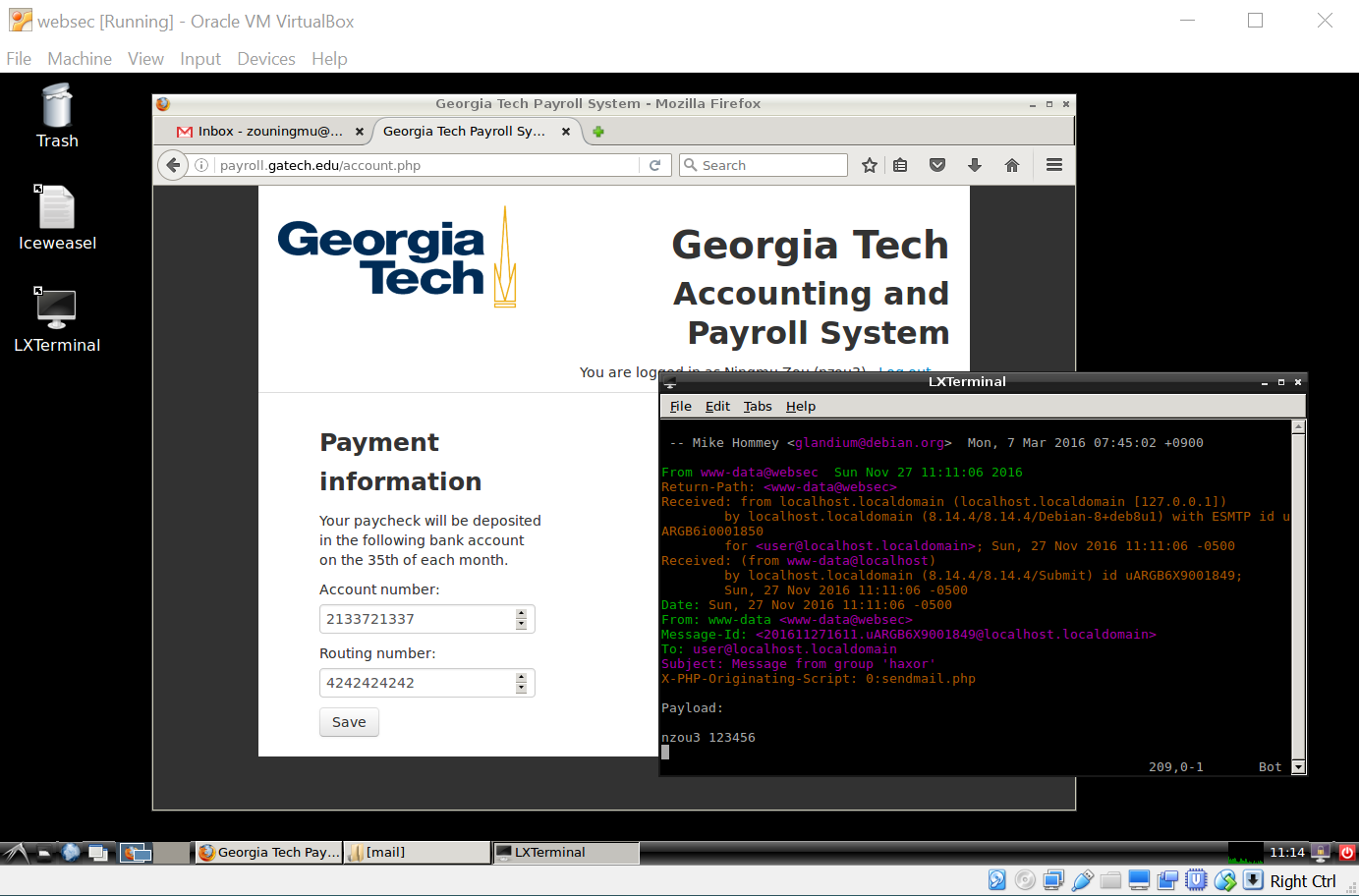


Target <2>

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.



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.

