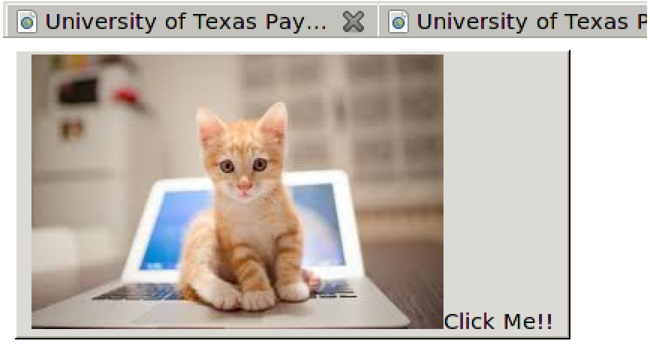
ASSIGNMENT - WEB EXPLOITATION

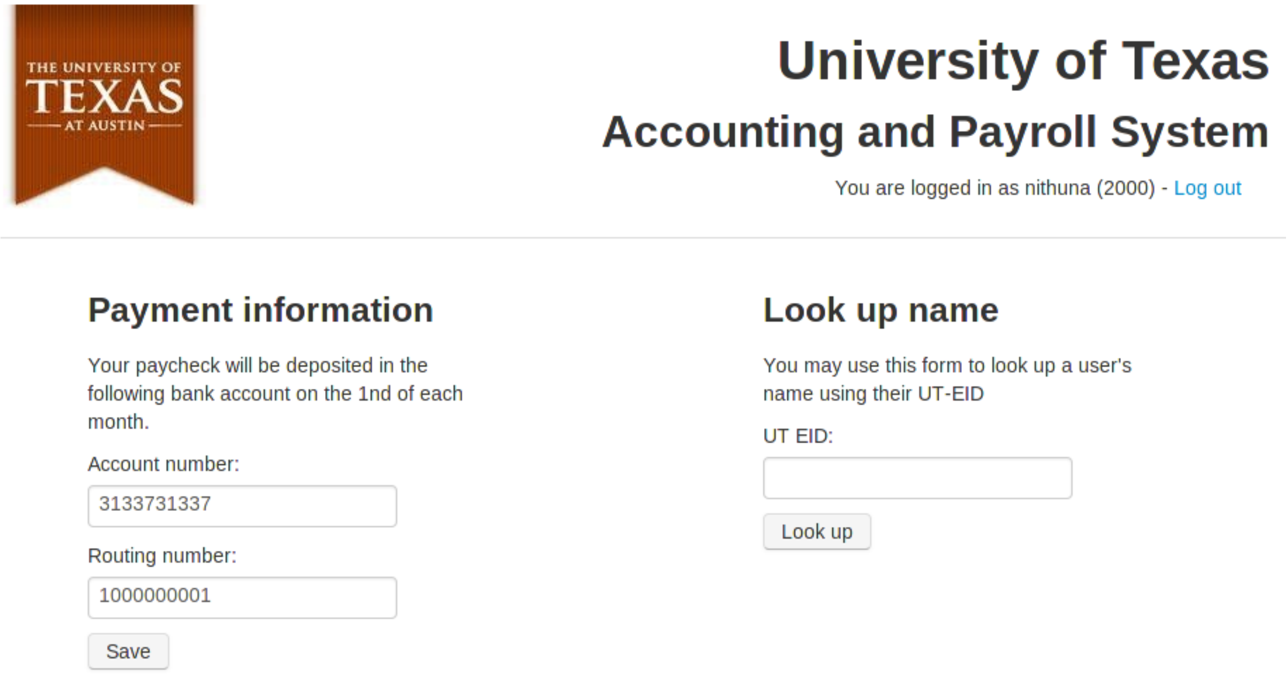
Submitted by,

NITHUNA PRAMOD PS
ANJU RAMDAS

Cross-site request forgery

When a victim has loggedin using the URL http://payroll.utexas.edu/index2.php, and then the victim visits the malicious page using the URL http://payroll.utexas.edu/Csrf.php. When the victim clicks on the picture of kitten or when he moves the cursor near to that picture then the victim's account number and routing number stored on the UT Payroll server will be changed to values 3133731337 and 1000000001 without victim's knowledge.





University of Texas

Accounting and Payroll System

You are logged in as nithuna (2000) - Log out

Payment information

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

Account number: 3133731337

Routing number: 1000000001

Save

Look up name

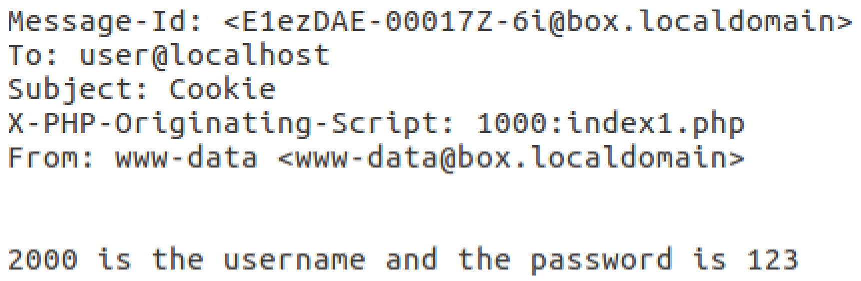
You may use this form to look up a user's name using their UT-EID

UT EID:

Look up

Password theft

When a victim enters the username and password and hits the Login in the page http://payroll.utexas.edu/index1.php , an email will be sent to user containing the username and password entered by the victim and shows loggedin as normal. The username and password are send by using the function mail() in index1.php

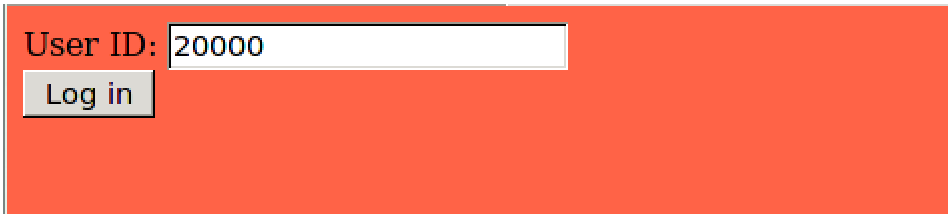


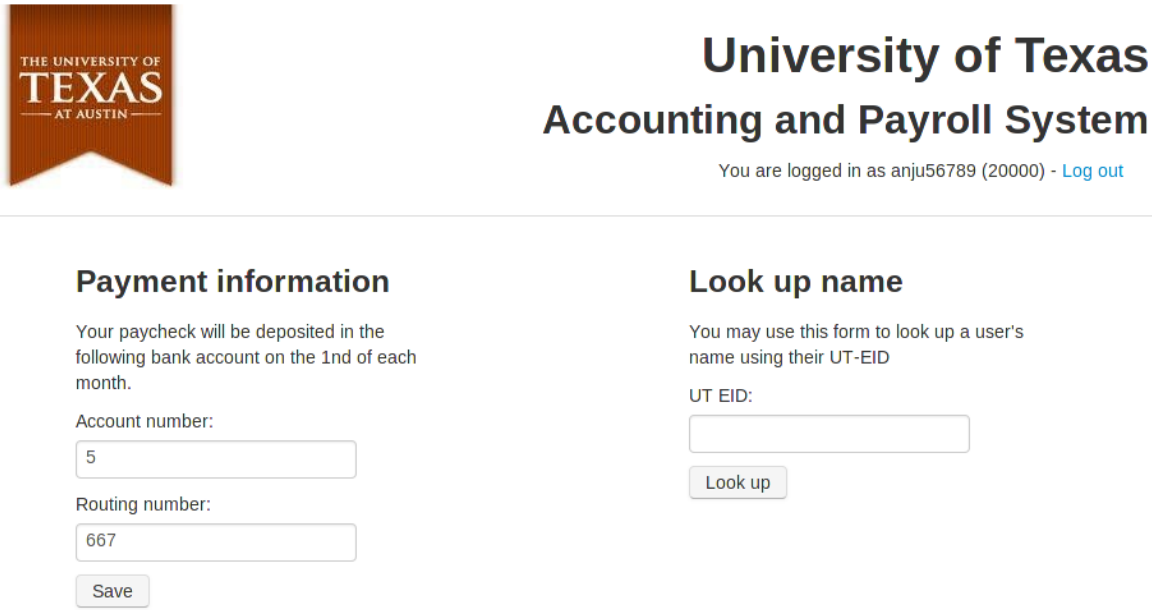
```
Message-Id: <E1ezDAE-00017Z-6i@box.localdomain>
To: user@localhost
Subject: Cookie
X-PHP-Originating-Script: 1000:index1.php
From: www-data <www-data@box.localdomain>


2000 is the username and the password is 123
```

SQL injection

A tester could login to a registered user’s account by just typing the userid on http://payroll.utexas.edu/sql.html. When the tester enter userid and press Login button, the SQL query, “'union select user_id, name, eid FROM users WHERE eid='$username';";//"” is appended with the userid. Then this userid is registered using register function in auth.php.

Then the same userid is passed to login function in auth.php. This appended userid replaces the $username in the line “$sql = "SELECT user_id, name, eid FROM users WHERE eid='$username' AND password='$hash'";” of login function. Thus without password the tester could login.


User ID: 20000



THE UNIVERSITY OF TEXAS AT AUSTIN

University of Texas

Accounting and Payroll System

You are logged in as anju56789 (20000) - Log out

Payment information

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

Account number: 5

Routing number: 667

Look up name

You may use this form to look up a user's name using their UT-EID

UT EID: