BugBusters – Security Vulnerabilities

This report discloses two security vulnerabilities by me (Santhosh Tuppad). These bugs need to be fixed as soon as possible because the facebook game app is already live and there have been 22,000+ likes and it is spreading.

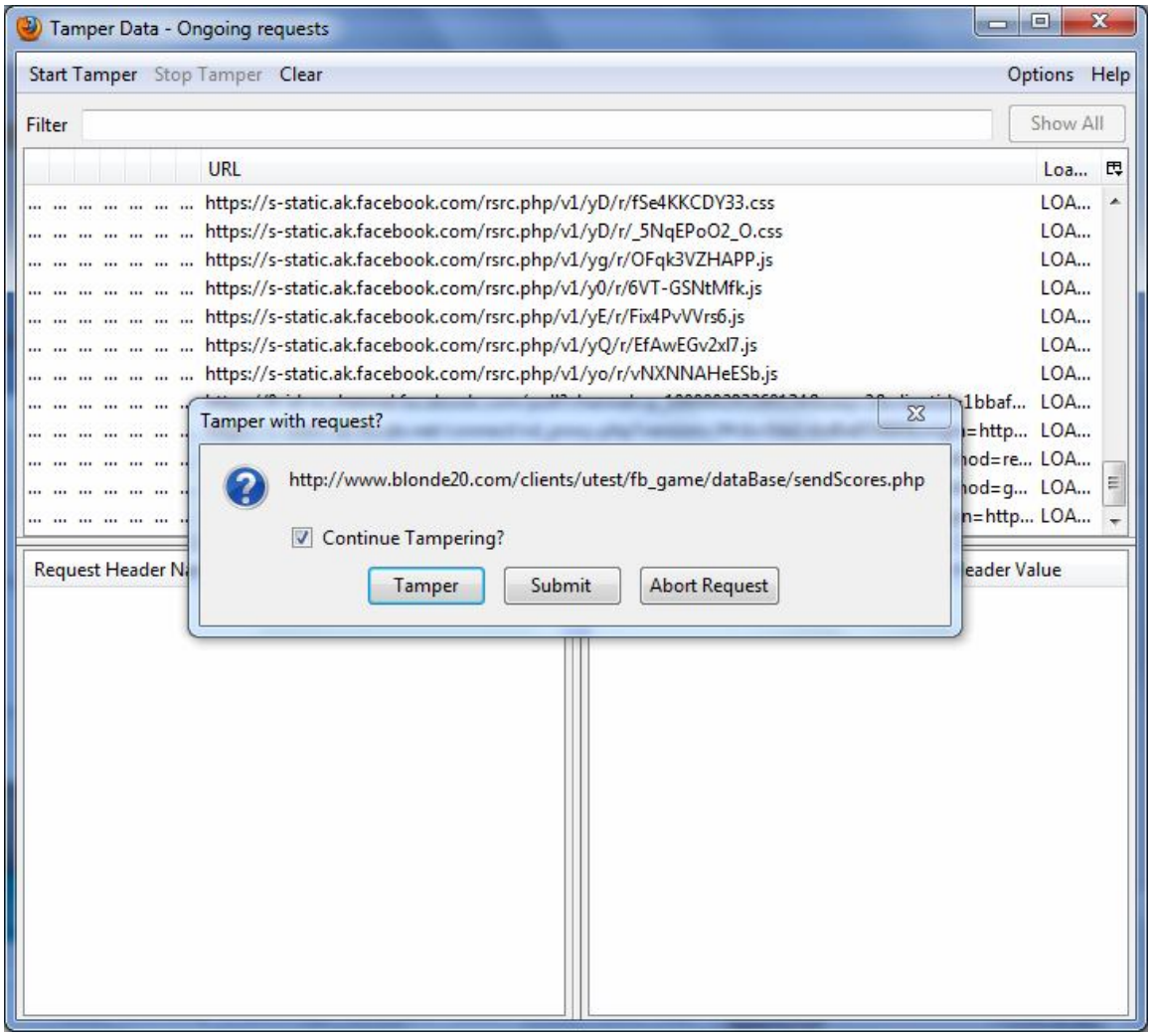
Security Bug #1

By tampering the sendScores.php POSTDATA it is possible to change the score to any value

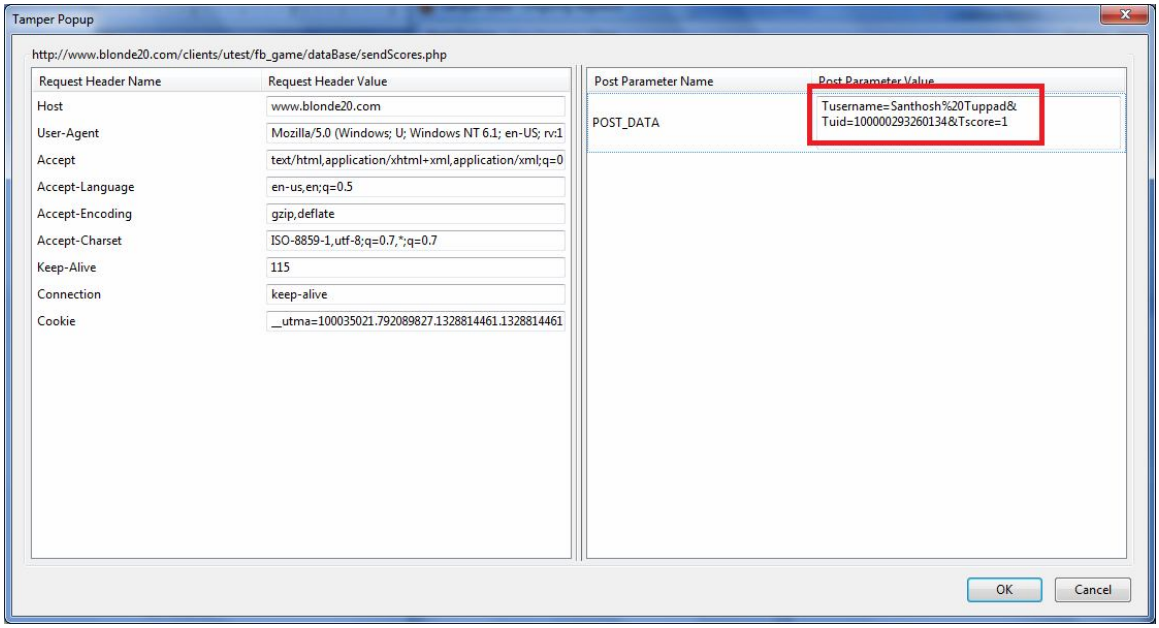
Below are the details of how you could reproduce it.

For this you got to use Mozilla Firefox 3.6.25 along with Tamper Data add-on installed on it.

1. When you are in BugBusters game webpage, start Tamper Data from "Tools" menu of Mozilla Firefox web browser
2. Now, do not play the game. Just wait till 3 attempts are over and game gets over.
3. Once game gets over you start finding Tamper Data waiting for you to tamper the requests.
4. Do not tamper any requests, till you see a request to tamper sendScores.php



5. Click on “Tamper” button and edit the values of score in POSTDATA text area as you see below,



Please zoom in and see the image details.

Now, a hacker to win the game could change the score=1 to score=1000 or any value to win the first prize, or second prize, or third prize or all the prizes.

Once you edit the score click on “OK” button and there you go. You are the winner now without playing the game.

How could hacker get all the three prizes?

There are three prizes that uTest is giving to the winners. Now, hacker could tamper all the 3 values accordingly to win 1st, 2nd and 3rd prize. He / she could ask 2 of other friends to receive the prizes while he / she tampers with it.

Hacker need not even login and then tamper. If you see in the tamper POSTDATA text area, there is “Tusername=Santhosh%20Tuppad” parameter. I just need to use my login itself and then provide the name of the other 2 friend’s profiles.

Now, you see how hacker can just win iPad2 and other two prizes.

Security Bug #2

readData.php shows all the history of the plays to anyone which should not be allowed

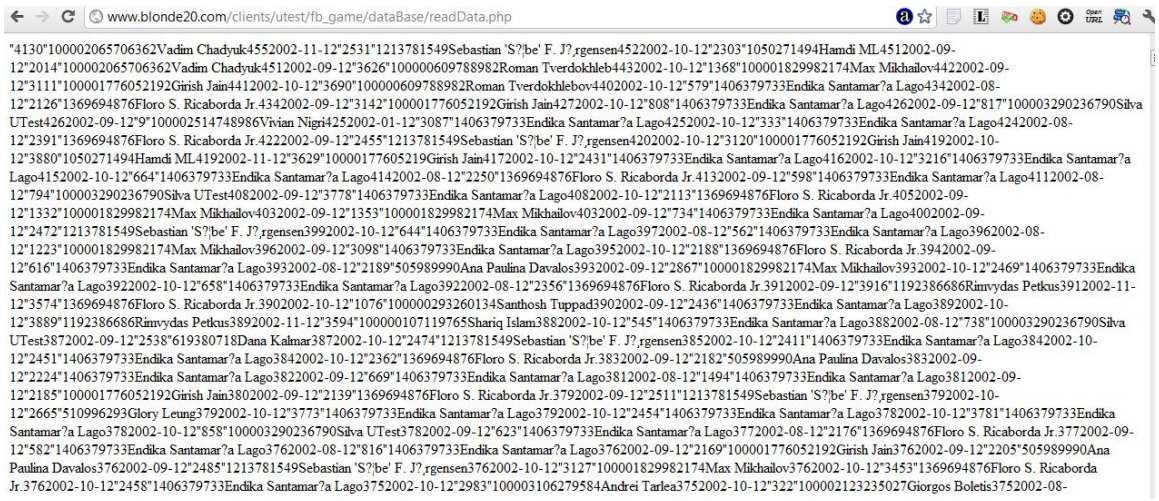
While monitoring the HTTP requests I see that readData.php is one of the request while high scores are being fetched. However; by using the following URL;

http://www.blonde20.com/clients/utest/fb_game/dataBase/readData.php Anyone can just navigate to this URL and see all the following details,

a. Username

b. Facebook Profile ID
c. Play ID
d. Date (Even date looks like it is set to 2002)

Below is a screenshot of readData.php



This data is not supposed to be shown to others because some users do not share their score on the facebook wall. It means that they do not want others to know their score or they do not want others to know that they played this game. But, access to readData.php doesn't protect their PRIVACY.

About Santhosh Tuppad

Director and Senior Tester at Moolya Software Testing Pvt. Ltd. (http://moolya.com/)

Over the last couple of years, Santhosh Tuppad has come to be known for his testing skills, winning bug battles & testing competitions across the world. He is a white-hat hacker and avid blogger at http://tuppad.com/blog/ & has authored many articles for various testing e-magazines.

For more details please contact me,
Twitter: @santhoshst
LinkedIn profile: http://in.linkedin.com/pub/santhosh-tuppad/12/b74/338

_END_OF_REPORT_