Client Side Security - Is it really a security?

Contributed by Aminur Rashid
Sunday, 22 May 2016
Last Updated Monday, 23 May 2016

I am sure we all must have read a number of blogs that recommend NOT to rely on client side security, and instead used Server side security. Yeah there exist other blogs also that recommends, strengthening your client side security. But the general (and rightly so) recommendation is to go for server side security. That is thumb rule.

I bring in my views on the topic. First things first. I hate to use the word "security" when it comes to client side. It is NOT a security. Not at all. It is as secure as the text you wrote in postcard. Remember?

To give more illustrations via image, if you call Client Side "security" as security, then it is as secure as these fences shown below:

Image courtesy: A key word "gate no fence" from google search

Calling anything related to restrictions on client side as security is just a farce. It must be stopped.

Why I am writing this blog?

Recently I was playing a virtual game on the website of one of the richest sports body of the world. Its an usual virtual game, where players compete against each other, they get limited substitute to be used for the entire tournament, they score points and in the end of the tournament, they get prizes. To my surprise, I found the website as one of the poorly designed website (I am not talking about the UI).

Client side Security Validation/Issues they had:

- They exposed the hidden "public" id of each team in the URL. Exposing an identifier for a team is not an unusual process, but then they were using this identifier in different update operations. Using this ID, anyone could have updated ANYONE's team.

- They had brilliant Client side Security to disallow a user from editing the team, once the transfer limit is reached. But since it was Client side Security, it was no Security at all and was just a matter of time for others to figure it out

Tools I used

Nothing. Why to use it? It was a plain website, and website runs on browser. So just use the browser. Chrome and firefox has one of the best Javascript debugger tool. Use it.

Steps:
1) The brilliant Client side Security I was talking about, was based on an attribute ("transfer-left"; obfuscated name) in the

html page. Right click on browser, inspect, edit the attribute and change the value from 0 to any number you want. There you go, you can transfer players (on UI) even if you have reached the limit.

2) Once you have completed the team, (if you are using Chrome) go to network field, and track the URL that comes once you submit the data.

3) Since they already implemented a brilliant Client side Security, they cared "mildly" about server side validation. So this mild validation will return you an error saying limit has reached. But then the URL you saw after submitting the data, in step 2 above, gives you enough lead that they have provided an option for "back-door" entry (not sure why? Probably they were sure that their site will crash again and they will give amnesty to players and will allow them to submit team even after exhausting the substitutes). Just toggling the value of a query parameter of the url (got from step2 above) and resubmitting it, resulted in successful submission.

Why I am writing this now?

I wanted the tournament to be over, or at least league rounds be over so that no one else can get past the "Secured" gate (And I will be surprised if no one else would NOT have noticed it).

I played for sometime to highlight the mistake, and I am stopping after the league round so genuine player wins in the end. I am also tweeting to the board head and board to see if I can get their response and a chance to visit their office, office of the one best sporting board of the world.

Note:
When the tournament started, the website used to crash near to the daily cut-off time to select a team. This used to happen because a lot of players selectz team at the last moment. This saves them from selecting a player, who was not playing that day. They (poorly) resolved the issue, by extending the cut-off time to post start of the match. I think an excellent sporty body like this deserves a better IT team. Much better team.