Homework#2 [35/100 points]

Assigned: February 23, 2018
Due: March 9, 2018

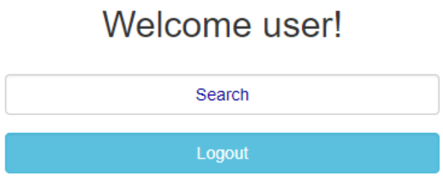
Important Note: You are required to find flaws/vulnerabilities **manually**. The only tool that you are allowed to use for this task is a HTTP proxy tool, e.g. Burp Suite, Zed Attack Proxy, WebScarab to analyze and modify HTTP responses & requests ONLY. **No** other tools are allowed, especially those that can cause denial of service to the system. Brute-force attack is not necessary for this task.

Also, do not make any modifications to any data in the system if not required from the task, e.g. do not change password, change data in the tables, delete tables or drop a database. The system is especially modified and deployed for learning purpose only. The company and all the employee names described or in the system are fictitious.

You are assigned to find vulnerabilities and attack a simple HR web application system with a limited functionality. This web application allows users and administrator(s) to view and search for employee names and details. No one should have access to users' passwords and other sensitive information. An administrator can also add new employee records to the system. The URL of the web application is http://www.myvulnerablesite.com/learn/.

Task 1 - Breaking into the system and gaining unauthorized access to information [15 points]

1) [3 points] A username/password is required to access the HR web application system. However, you do not have one. Your task is to exploit the web's authentication mechanisms and gain access to the system. After you successfully authenticate yourself, you will be displayed with a welcome page like the one shown below and/or be able to access other pages of the web. Explain the approaches used to gain unauthorized access to the system. Also, identify three vulnerabilities that you can take advantage of to gain unauthorized access to the system.



Welcome user!

2) [2 points] For each vulnerability identified in Q1, explain how you would remove such vulnerability and improve the security of the system.

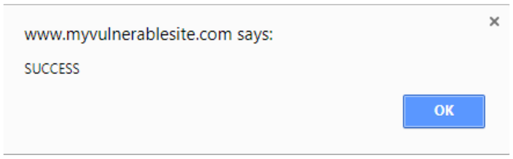
3) [1 point] After you have successfully logged in, go to the 'search' page. The search page queries a list of employee names based on the inputted keywords. Identify a possible SQL statement used for this query.

4) [2 point] The next task is to use SQL injection to display all the names of the employees in the web application, how would you achieve this? Explain how you achieve this with step-by-step screenshots.

5) [2 points] Your task is now to get hold of ALL employees' social security numbers. The social security numbers are stored as a 9 numerical digits. How would you do this? Explain how you achieve this with step-by-step screenshots.

6) [3 points] You would also like to get hold of the username and hashed passwords of the user and admin accounts of the web application. How would you accomplish this task? What are the username and hashed passwords for all the accounts? Explain with step-by-step screenshots.

7) [2 points] If logged on as a regular user (using an account identified in Q6 in a 'user' group), can you find way(s) to gain elevated access to a resource that is protected from users, i.e. to access an administrative function? For this, you must identify a page that only an admin can perform the administrative function. Explain in detail how the privilege can be escalated. You should be presented with a pop-up window that says 'SUCCESS', if you can successfully perform the administrative function as an admin.


www.myvulnerablesite.com says:

SUCCESS

Task 2 – Attacking the users and the web application [11 points]

8) [2 point] Identify <u>two</u> entry points that are vulnerable to a cross-site scripting attack. Explain in detail on how the vulnerability is detected.

9) [1 point] Out of the two entry points that you identified in Q8, which one would you choose to use as part of a social engineering attack. Explain.

10) [5 points] From Q9, craft a link so that when it is clicked by a victim, he/she will be presented with a page that asks for the site's user login and passwords. The page should <u>not</u> be redirected to somewhere else. The URL shown in the browser needs to begin with 'www.myvulnerablesite.com/learn/'. When the login credentials are entered or submitted, they will be sent to the attacker's side. The attacker's side must be able to receive requests sent from the page. You can implement this part by any means and in any web programming language you prefer. You also need to create a web page that can display the IP of the victim and the inputs captured. For this task you may need to pay some (small) fee to host your web, if you don't already have one.

You need to submit the link to be submitted to a victim, and the link on how to access the attacker's web page. Full points will be given when login credentials (from the victim browser) can be displayed on the attacker's website that you provide.

11) [3 points] For the threats/vulnerabilities that you identify in Q8-10, explain in detail how this can be prevented by a developer and by a user of the website.

Task 3 – Threat Modeling & Risk Analysis [9 points]

12) [6 points] Perform a threat modeling for Etsy (https://www.etsy.com/), a global marketplace that sellers and buyers can connect and exchange goods on the platform. Limit your analysis to the following features:

    - Selling & buying of goods / providing reviews / processing of payment

    The deliverables include: a level-1[1] Data Flow Diagram (DFD) of the system and list of threats identified using STRIDE-per-element. You should come up with several threats in each STRIDE category.

13) [3 points] Draw an attack tree[2] for one threat identified in Q12 that you think that has the highest risk. Explain also why you think so. Your attack tree should show different ways to accomplish the attack goal.

This homework is to be done individually. You must write your answer *independently*.

To submit an assignment, log into home.nyu.edu, go to Academic -> NYU Classes -> Special Topic: Practical Computer Security -> Assignments, and upload your answer in PDF format. Make sure that you 'submit' the assignment before the deadline.

Late homework will be marked down by 20% for every day of lateness.

[1] You can refer to https://www.visual-paradigm.com/tutorials/data-flow-diagram-example-food-ordering-system.jsp and the additional slide provided for some explanation of level 1 DFD.

[2] More information on attack trees can be found here: https://www.schneier.com/academic/archives/1999/12/attack_trees.html