IT-Security 2019

Exercises: Web Security

Exercise 1: SQL-Injection

The URL given below leads to a demo website of the fictional bank *Altoro Mutual*. It is deliberately designed to be vulnerable.

1. **Use a SQL-Injection to log in as user admin and answer the following questions:**

    1. **How can you circumvent the check for a correct passw ord?**
    2. **How does the WHERE clause of the SQL statem ent used for the login look like?**
    3. **After you successfully logged in: How can you use a SQL-Injection to show allrecent transactions of allusers?**
    4. **Is the vulnerability susceptible to *normal* SQL-Injections or to *blind* SQL-Injections? Justify your answ er and state the difference between the two.**

Weblink: http://demo.testfire.net

Exercise 2: Cross-Site Scripting

The Altoro Mutualbank is also susceptible to Cross-Site Scripting (XSS) attacks.

1. **Look for a place, w here you can conduct a reflected XSS attack against a user that is currently *not logged in*.**
    1. **Design an attack that fakes the Login form to attack users that are currently not logged in. Send the login inform ation to a server of your choice and login the user normally afterwards.**
    2. **How can you hide the attack code to the victim? Implement an exemplary concealment.**
2. **Look for a place, w here you can conduct a reflected XSS attack against a user that is currently *logged in*.**
    1. **Design an attack that reads inform ation about the user and send it to a server of your choice.**
3. **What would be your advices for the Altoro Mutualbank in order to close the vulnerabilities or to make exploiting them impossible?**

Weblink: http://demo.testfire.net

See page 2 for further exercises!

Exercise 3: API Information Disclosure

The URL given below leads you to the SRH Student Mood Board. It is a fictional application which allow s logged-in SRH students to post a short message on a board either with their name or anonymously. The user interface is developed to not reveal the name of the student if they decided to post a message anonymously. You will find that someone posted a m essage saying that he or she already solved all exercises for IT-Security. Unfortunately, this user decided to post this message anonymously.

1. **Find out the name of the student who posted the m essage and explain the steps you perform ed to reveal it?**
2. **What is your advice to the developer of the SRH Student Mood Board to close the information disclosure?**

Weblink: https://bit.ly/itsec-w3-e3

Exercise 4: Web Security in Practise

Develop a sm allw eb application in a programming language of your choice that initially is deliberately vulnerable to one of:

- **SQL-Injection, or**
- **Cross-Site Request Forgery, or**
- **Rem ote Code Execution**

Explain where and why your code is vulnerable to the selected vulnerability and develop a fix for that. You can either subm it the com plete source code of your self-developed program (unfixed and fixed version) or (preferred) you create a repository on github.com w hich contains at least tw o com m its (initial commit + commit which closes the vulnerability).

Hint: If you don't know w here to start you can have a look at one of the following tutorials that supports you in creating a skeleton for a web server and web content:

- Node.js: https://www.tutorialspoint.com/nodejs/nodejs_express_framework.htm
- Python: https://realpython.com/blog/python/primer-on-jinja-templating/
- Java: https://spring.io/guides/gs/serving-web-content/

Exercise 5: Cross Origin Resource Sharing

In the context of *Cross Origin Resource* is. Also explain when and why it's used explanation. *Sharing (CORS)* explain in your ow n words what a *preflight request* by browsers. Preferably, use diagram s and/or code snippets for your explanation.

Reminder: Always cite all your sources!