Project Guidelines

Fabrizio M. Maggi
maggi@inf.unibz.it

How many people in a group?

- Groups of **max 3 people** are allowed.

Which programming language?

- Java.

What is it provided to you?

- The application provided is a web application that allows: (i) login management; (ii) reading, sending and receiving e-mails using a web server Tomcat.
  - The application is provided at: https://github.com/francxx96/ExamProject
- The application is totally “insecure”.
- The application is provided mainly for two reasons:
  - To be used as a common guideline showing how the application should work.
  - To provide an example of a web application developed without “security awareness”.

Goals

1. Prepare a demonstration of how the provided application can be hacked. It is required to demonstrate attacks **at least** based on (i) SQL injection; (ii) XSS reflected; (iii) XSS stored; (iv) XSRF. In addition, you are **free to show additional vulnerabilities** of the provided application.
2. Implement a “secure” version of the provided application implementing protection mechanisms to deal with the vulnerabilities found in point 1 (at least the ones in (i)-(iv)). You are free to implement **the protection mechanisms in whatever way**, with the only requirement that the **programming language must be Java**. For preventing password theft, a **mechanism based on salt values/hashing** should be implemented.
3. Prepare a demonstration of how the secure application **can no longer be violated** using the attacks that were previously successful (in point 1).

Goals

4. Implement a mechanism to **encrypt and digitally sign the (body of the) emails sent** (using RSA, and any method to map characters and integers, e.g., using ascii tables). This should be implemented as follows:
   a) When a user registers, a key pair is generated and stored **on the client side**.
   b) Before an e-mail is sent, it is **always** encrypted with the public key of the receiver (that should be retrieved somehow by the sender).
   c) An e-mail can be digitally signed **only in case the sender decides to do so**.
   d) When an e-mail is received, it is decrypted with the private key of the receiver.
   e) If a received email is digitally signed, the digital signature is checked (to do this the public key of the sender should be retrieved somehow by the receiver).

Remind that the **private key** should never leave the node in which it was generated.

Goals

5. *Pentest*: Attempt (which may or may not be successful) to violate a “secure” application implemented by another group. **Any kind of vulnerabilities can be found**.

What to submit? (goals 1-4)

- **GitHub repository** containing the developed application.
- **Brief user manual** for installation and use of the application.
- **Screencast** containing a demo that illustrates (i) how the application is used in a standard scenario (including the case of emails digitally signed); (ii) how the “insecure” application can be violated; (iii) how the “secure” application does not allow violating the application using the same attacks as in point (ii); (iv) ***the parts of code where you have implemented the security mechanisms*****.**

What to submit? (goal 5)

- **Screencast** containing a demo of the attempt (successful or not) to violate the application of another group.

How to do the screencasts?

- The submitted screencasts should be video recordings with audio (with the voice of at least one member of the group presenting).
- The screencasts can be put online or sent via e-mail and there is no time limitation as far as the presentation contains all the information required (*including a description of the parts of the source code implementing the security mechanisms*).

When to submit? (goals 1-4)

- Submission by **05 June 2022, 23:59 CET**

When to submit? (goal 5)

- Submission by **14 June 2022, 23:59 CET**

How to submit?

- Send the manual and the (links to the) screencasts **via email** to **maggi@inf.unibz.it**
- The GitHub repository can be public (in this case please send me the link to **maggi@inf.unibz.it**) or private. In this latter case, you can send me an invitation at **f.m.maggi@ut.ee** (username fmmaggi).
  - It is not possible to make changes to the repository after submission.
- When you send me the material via e-mail, please specify in the e-mail the names of all the members of the group.

Project Discussion

- The project will be **discussed individually** during the oral exam.

Grade

- **The project will contribute 30% of the final grade.**