LUNDS UNIVERSITET
Lunds Tekniska Högskola

EITF05 Web Security
Functionality Review Form
Autumn 2019

How to perform the functionality review

The functionality review takes the form of a role play. The group that performs the reviewing represents a company (denoted ‘Company’ below). The Company has ordered a secure web shop from a subcontractor (denoted ‘Subcontractor’ below). The Teacher acts as an expert hired by the Company.

The Company wants to assess the security of the design and the implementation. The primary goal of the Company is to acquire a secure product with the specified functionality. The secondary goal is to pay the Subcontractor as little as possible. This can be accomplished by finding security problems, either in the software or with the competence of the Subcontractor employees themselves. Anything that contributes to decreasing the credibility of the Subcontractor is of value in this sense, from finding actual errors in the design or implementation to discrediting the Subcontractor employees.

The Subcontractor’s goal is to get paid for their work. Even though they have a contract, they still need to motivate that they have fulfilled their part of the agreement.

Each subcontractor employee has one of four different types of roles;

1. Chief architect,
2. Chief security analyst,
3. Chief tester and
4. Senior developer.

Each is responsible for answering the questions most relevant to their domain. These roles are assigned according to the group member count (from left to right) of the group member listing on the course home page. Prepare answers for your questions. If your group has only three members, the fourth role is handled by all members together.

The review process is as follows.

1. Senior developer and Chief analyst demonstrate that their SSL connection works.
2. Subcontractor demonstrates that the password handling is implemented according to specification.
    a. Chief architect motivates that the password policy is reasonable.
    b. Chief architect and Senior developer show and motivate the easy-password blacklist functionality.
    c. Tester shows that credential storage is explicitly protected against SQL-injections.
    d. Chief analyst shows adequate security against on-line brute-force attacks.
    e. Senior developer motivates and shows the protection against TMTO / Rainbow attacks.
3. Senior developer demonstrates that the usage of PHP sessions is reasonable.

4. For each attack that has been implemented, do the following.
    a. Chief architect and Chief analyst together explain to the Company how the attack works in general.
    b. Tester demonstrates (use-case and code) how their website can be made susceptible to the attack.
    c. Senior developer demonstrates how they explicitly protect their website so that the attack no longer works.

Note that there is a time limit of 25 minutes for the review process. If you are not able to comfortably (you are at a business meeting, not at a world championship speed-talking convention) complete the above specified review process within this time, you need to make a new booking for another functionality review. So in order to avoid unnecessary work – come prepared!

LUNDS UNIVERSITET
Lunds Tekniska Högskola

EITF05 Web Security
Functionality Review Form
Autumn 2019

Functionality review report

The teacher fills out the relevant information in this section.

Company group number: Subcontractor group number:

Attacks implemented and reviewed:
□ SQL Injection
□ Remote File Inclusion
□ Cross-Site Scripting (XSS)
□ Cross-Site Request Forgery (CSRF)
□ CSRF token bypass using XSS

The Company hereby confirms that the project implementation of Subcontractor is of sufficient quality and complies with the project requirements.

Company signatures:

Teacher signature:

Pegah Nikbakht Bideh
Lund, 2019 - 10 - ___