UNIVERSITÄT BONN

Secure Software Engineering

Exercise Sheet code, Winterterm 25/26

We highly encourage you to do the assignments yourselves, as all the exercises are relevant for the exam. It is also recommended to visit the tutorial, as there will be a discussion about the exercises, not just the solutions. For the *Vulnerability of the Day* exercises, we recommend examining the code snippets, if any, while conducting your research. Keep in mind that the entirety of the lecture is relevant to the exam. If a topic or some details are not specifically talked about or mentioned in the exercises, that does **not** mean that it will not be part of the exam!

If you have any questions, please do not hesitate to ask your tutor Aura, Kati or Lukas. (Hint: the mails are embedded in the names.)

Good luck and have fun! :)

This sheet aims to give you an idea of what you can expect in the exam related to the Vulnerabilities of the Day and defensive coding. In general, you should be able to understand the workings of these vulnerability types to identify possible problems in short code snippets (up to 25 lines) in common programming languages (Java, Python, PHP). All important function calls will be explained with comments in the code.

Example 1

The following Java code snippet may contain one or more coding mistakes that violate defensive coding guidelines.

Your task is to:

- Identify the line with the mistake. (1 Point)
- State the issue briefly. (1 Point)
- Describe the mitigation briefly. (2 Points)

If there is no coding mistake in the snippet, state this and briefly explain why.

Note: Syntax errors do *not* count.

```
1  public boolean verifyPassword(String user, String password) {
2      if (password.equals("") || password.length() < 16) {
3          return false;
4      } else if (!password.matches("[^a-zA-Z0-9]*")) {
5          if (password.equals("bBc$3FRab#%V(@9VvL7")) {
6              return true;
7          }
8          if (checkPWForUserSecure(user, password)) // Assume this is a secure
9          //implementation of a password check
10             return true;
11     }
12     return false;
13 }
```

Example 2

The following PHP code snippet may contain one or more coding mistakes that violate defensive coding guidelines.

Your task is to:

- Identify the line with the mistake. (1 Point)
- State the issue briefly. (1 Point)
- Describe the mitigation briefly. (2 Points)

If there is no coding mistake in the snippet, state this and briefly explain why.

Note: Syntax errors do *not* count. Wrong answers get a 4-point deduction. q

```
1  <!DOCTYPE HTML>
2  <html>
3  <body>
4  <?php
5      $template = 'fancy.inc';
6      if (isset($_GET["theme"]))
7          $template = $_GET["theme"];
8  // include() function is used to load the contents of another file here
9      include("themes/" . $template);
10     echo makePageContent();
11 ?>
12 </body>
13 </html>
```

In PHP, variable names are indicated with a $-character. `$_GET` is an array that contains all GET parameters passed with the request. For example, if a site is called like this:

```
https://site.com/index.php?id=1
```

then `$_GET["id"]` would contain the value `1`.