CS161–Spring 2015 — Solutions to Homework 2

Quoc Thai Nguyen Truong, SID 24547327, `cs161-di`

April 12, 2015

Collaborators: God

Problem 1

(a)

$$c'_2 = 0 \quad , \quad d'_2 = 0$$
$$c'_{3t} = c_3 \quad , \quad d'_{3t} = min(d_3, b_3)$$
$$c'_{3f} = max(a_3 + 1, c_3) \quad , \quad d'_{3f} = d_3$$
$$c'_4 = c_4 \quad , \quad d'_4 = d_4$$
$$c'_5 = c_5 + 1 \quad , \quad d'_5 = c_5 + 1$$

(b)

$$c_3 = min(c'_2, c'_5) \quad , \quad d_3 = max(d'_2, d'_5)$$
$$c_6 = min(c'_{3f}, c'_{1f}) \quad , \quad d_6 = max(d'_{3f}, d'_{1f})$$

(c) The vulnerability of the function is $\boxed{Off\ By\ One}$

Problem 2

(a) $\boxed{Failsafe\ defaults}$
The default is not unsafe to give $300 to customer without checking card is valid or not.

(b) $\boxed{complete\ mediation}$
It should check for authority in every users/objects before let them access the web.

(c) $\boxed{Security\ through\ obscurity}$
A system relying on security through obscurity may have theoretical or actual security vulnerabilities. Since the duress code is known through public documentation, the attacker can find and attack.

(d) $\boxed{Least\ privilege}$
The SuperFlashlight controls and access the information and recourse that are not necessary for legitimate purpose.

Problem 3

(a) $\boxed{NO}$
Since Bob does not have root access, so he can't execute escalate.c .

(b) $\boxed{YES}$
Since we know that other users can able to run the file with the privileges of the owner, Bob will able to execute escalate.c .

(c) $\boxed{YES}$
Once he got the path of the file, he can call new_event on that path so that it can make a copied of the file and execute escalate.c .

Problem 4

(a) $\boxed{False}$
It can be very effective but cannot defend against malware unless some of its samples have already been obtained, a proper signatures generated and the antivirus product updated. Also, this does not really effective against zero-day or next-generation malware.

(b) $\boxed{True}$
Advertising, by definition, is ceding control of Web content to another party

(c) $\boxed{False}$
Rootkit is a set of trojan system binaries.It can install hacked binaries for system programs such as netstat, ps, ls, du, login

(d) $\boxed{True}$

Problem 5

Repeat "http://browsertest.com/?u=" after "/?u="
http://browsertest.com/?u= http://browsertest.com/?u= http://browsertest.com/?u= ...

If there are n repetitions and n is large, BrowerTest will make 2^n HTTP requests. Therefore, this will overload the BrowerTest server.

Problem 6

1. (a) $\boxed{Blacklisting}$
   +One Advantage: it is conceptually simple to recognize a few bad things(virus, malware), stop them, and allow everything else.

   +One disadvantage: Very hard to capture the malicious string as we can see in the project, and it's not a good practice if it allows attacker to use an attribute from html form to perform an XSS attack.

   (b) $\boxed{YES}$
   Example: If an attacker entering malicoous user-name which contains "scrscriptipt....", the library will remove substring "script". Therefore it becomes "script..." .

2. (a) This is Cross Site Request Forgery (CSRF) vulnerability, or one-click attack. Eva stole one dollar from me by let me click on the tinyrul and the Tinyrul redirect to:
   http://www.cashbo.com/payment?amount=1&recipient=Eve
   Now, I lost 1 dollar.

   (b) For every transaction, we should ask the user to re-enter their username and password to make sure that he/she is authorized current user.

Problem 7

```
a)
username = "';DROP TABLE

b)
username = admin"'--

c)
username = "\';DROP TABLE


d)
PreparedStatement psmt = conn.preopareStatement("SELECT user_id FROM Customers WHERE
                                                 username = ? AND password= SHA1(?)");
pmst.setString(1,username)
pmst.setString(2,password)

Explain:
Prepared statement only accept one parameter at a time.
setString get only 1 string at a given time, and it won't parse
any SQL code within the parameter.
```

e)

Problem 8

Great!!!