CORPORATE COMPUTER SECURITY

CHAPTER 8: APPLICATION SECURITY

LAB ASSIGNMENT ON CHAPTER 8

PROJECT 1

Buffer overflows are a fairly common vulnerability. They can crash an application, allow unauthorized people access, process unintended payloads, and so on.

1. Open a web browser and go to http://nsfsecurity.pr.erau.edu/bom/.
2. Scroll down and click on the link labelled "Spock."
3. Click Play.
4. After it stops, enter the first eight characters (ONLY 8 characters) of your last name as the password. (If your last name has less than 8 characters, you can fill in the last characters with "X." For example, "Boyle" would become BOYLEXXX.)
5. Click Play.
6. Click Reset.
7. Click Play.
8. After it stops, enter the first eight characters (ONLY 8 characters) of your last name as the password AND add the letter "**T**" at the end. (If your last name has less than 8 characters you can fill in the last characters with "X." In this case, it would be BOYLEXXXT.)
9. Click Play.

Questions

1. In the buffer overflow project above, why did the addition of the letter "T" allow you to bypass the login with a fake password?

2. What would happen if you entered a 15-character password consisting of all Xs?

3. Could the code behind this login be fixed to stop this buffer overflow? How?

4. Are there different overflow attacks? (Hint: Look at the other examples shown.)

Further questions

1. What is a concurrency flaw?

2. Have most real websites taken measres to secure their systems against concurrency flaws?

3. What is cross-site scripting?

4. Could a subcontractor with weak security practices make a corporation more vulnerable? How?

5. How can organizations limit their exposure to malware?