Lab 1 -Attacking the Web Goat

Summary
WebGoat is a full-featured web application which is built from the ground up by the OWASP foundation to be very insecure! Let's attack WebGoat to explore some common web attacks.

We will attack WebGoat using Tamper (A Firefox extension).

Other fun tools such as BurpSuite and WebScarab could be used.

Lab 1 will let you execute the following attacks against the 'Goat!

1. Stored XSS
2. Improper Error Handling (Fail Open)
3. Numeric SQL Injection

Instructions

1. Open the "lab1" folder, which you have likely already done, since you are reading this PDF.
2. Start Firefox. You will see a WebGoat bookmark on the bookmark toolbar. Don't click it just yet.
3. Access WebGoat by clicking the webgoat bookmark on the Firefox bookmark toolbar. Start the training by clicking the "Start WebGoat" button.
   • http://localhost:8080/WebGoat/attack
4. Login with the credentials user guest, password guest
5. Note the Lessons on the vertical navigation section
6. Attack! (But first get to know your attack tools)

Tool Introduction

1. Navigate around the WebGoat application using Firefox. Make sure no proxy is set in the upper right hand portion of the toolbar.
2. Open the "Tamper Data" plugin and turn on tampering. Note that it hangs up any GET or POST operations until you tell it to continue. When you are done, turn off tampering and clear the console.
3. Other stools that could be used on your own time include:
   • Open up BurpSuite. Set your Firefox proxy to use BurpSuite. In the BurpSuite application, note the Proxy->Intercept page. Experiment with this. Browse some WebGoat pages.
   • Open up WebScarab. Set your Firefox proxy to use WebScarab. Try to find the same functionality as you just discovered in BurpSuite. Browse some WebGoat pages.
4. OK. Now we attack!
Attack 1 - Stored XSS

1. Access the stored XSS attack by clicking the "Stored XSS" stage:

2. Follow instructions on the attack and attack the application using stored XSS.
3. If after 10 minutes, you have not completed the stage, click on the "Solution" button on the gray nav-bar, far right. BE SURE TO STILL EXECUTE THE ATTACK.
1. Access the improper error handling attack by clicking the fail open stage:

2. The goal of this attack is to login without a valid password by creating an unhandled error condition on the back-end.

3. Hint: Click on the "Show Params" before logging in with a bogus password. What are the query parameters that are being sent from your browser to the web application?

4. Hint: What would create an 'error' on the backend? Hmm....What happens if one of the important parameters is omitted from the request?

5. Hint: I wonder how we could delete one of the parameters sent to the web app? Would a tool that allows us to intercept and remove a request help here?

6. If after 15 minutes, you have not completed the stage, click on the "Solution" button on the gray nav-bar, far right. BE SURE TO STILL EXECUTE THE ATTACK.
Attack 3 - Numeric SQL Injection

1. Access the attack by clicking the Numeric SQL Injection attack link:

2. The goal of this attack is to fool the web application to list data it should not. You will need to formulate a response which tricks the application in displaying all weather stations.
3. Hint: Look at the SQL on the page. How could you make that return all rows from the table and not just station = [station]? Is station ID being submitted? Hmm.....
4. Attack the app in **TWO WAYS**, getting the same result (all weather stations listed)
   a. Use Tamper plugin to modify POST parameters
   b. Modify GET parameters in the URL
5. If after 20 minutes, you have not completed the stage (using the three different methods), click on the "Solution" button on the gray nav-bar, far right. BE SURE TO STILL EXECUTE THE ATTACK.

Web Goat Bonus (If time permits) – More XSS and SQL Injection

Wrap Up Discussion
1. What damage could be done by exploiting a real web application?
2. How do end-users protect themselves?
3. How does a web application developer prevent these issues?
4. What skills does a web application developer need?
5. How to continue with WebGoat?