**WebGoat Exercise**

WebGoat is really good vulnerable web application to start with, because it contains lots of hints for beginners.

1. Injection Flaws. Simple SQL injections.

Injection ﬂaws allow attackers to relay malicious code through an application to another system. These attacks include calls to the operating system via system calls, the use of external programs via shell commands, as well as calls to backend databases via SQL (i.e., SQL injection). Whole scripts written in Perl, Python, and other languages can be injected into poorly designed applications and executed. Any time an application uses an interpreter of any type there is a danger of introducing an injection vulnerability.

a) In a Stage 1 tab: String SQL Injection try to login as an admin. (hint: Try to get use of Firefox Web Developer).

Please describe your solution here…

b) In String SQL section display all card numbers of all users.

Please describe your solution here…

c) Blind Numeric SQL Injection. Find the pin in the pins table for the cc number 1111222233334444 (SQLmap can be useful).

Please describe your solution here…

d) Log Spooﬁng. Login as an admin in this section. Check the login for also for possibility of XSS.

Please describe your solution here…

e) Can you ﬁnd all users that its name starts with letter ‘J’.

Please describe your solution here…

2. Cross Site Scripting (XSS) attacks.

Cross Site Scripting involves scripts being run by sites that reﬂect user input back to the browser‘s window without any context-sensitive output encoding. This results in code actually being executed instead of text being displayed.

a) Phising with XSS

Using XSS and HTML insertion.

i) Insert XSS and HTML credentials.

Please describe your solution here…

ii) Add JavaScript to actually collect the credentials.

Please describe your solution here…

b) XSS attacks

i) Check if the website is vulnerable for XSS attacks. Input script that will show an alert message. Present what does the output look like in your case.

Please describe your solution here…

ii) List 10 diﬀerent payloads that works on this site.

Please describe your solution here…

iii) Name few ways that the developer/programmer can avoid such a vulnerability.

Please describe your solution here…

iv) Steal the cookie of the session. Describe brieﬂy the way You did it. Send the cookie to some .txt ﬁle.

Please describe your solution here…

d) Cross Site Request Forgery (CSRF)

Describe how does CSRF work on a theoretical level. Present it in a form of a diagram and then: Send the email to a newsgroup. The email contains malicious code hidden in a image whose URL is pointing to dangerous request. In this type of attack your message will be stored so anyone will can access the message. Remember to set the title interesting to gather more victims.

Please describe your solution here…

3. XML injection

XML Injection is an attack technique used to manipulate or compromise the logic of an XML application or service. The injection of unintended XML content and/or structures into an XML message can alter the intend logic of the application. Further, XML injection can cause the insertion of malicious content into the resulting message/document.

Go to AJAX Security -> XML Injection  
Try to add more rewards to your allowed set of rewards by altering the response. Follow the hints on the website.

Please describe your solution here…

4. Directory Traversal Attack

A directory traversal attack is an exploit which allows attackers to access restricted directories and execute commands outside of the web server’s root directory.

Go to Access Control Flaws -> Bypass a Path Based Control Scheme.  
Using BurpSuite try to hack the access control mechanism and reach some additional ﬁle that is not in listed directory. You may search for WEBINF/spring-security.xml ﬁle

Please describe your solution here…