CMPSC 497C Lab10: Web App Hacking

## Configure Webgoat: a broken web app for security testing

The following actions are done in Windows!

1. Download Webgoat from: <http://code.google.com/p/webgoat/downloads/detail?name=WebGoat-5.4-OWASP_Standard_Win32.zip>
2. Right click to decompress the package, and you will have a folder of webgoat; next enter the folder, double click ‘**webgoat.bat**’ to start the service.
3. Now your webgoat is started; open the **Firefox** browser to test it, the URL is: <http://localhost/WebGoat/attack>
4. Login credential: guest:guest

## Configure Burp suite as a web proxy for your browser

go to the Firefox menu, click on Options, click on Advanced, go to the Network tab, and click on the Settings button in the Connection section. Select the "Manual proxy configuration" radio button. Enter your Burp Proxy listener address in the "HTTP proxy" field (by default, 127.0.0.1). Enter your Burp Proxy listener port in the "Port" field (by default, 8080). Make sure the "Use this proxy server for all protocols" box is checked. Delete anything that appears in the "No proxy for" field. Then click "OK" to close all of the options dialogs.

## Drills – Webgoat drills

|  |  |  |  |
| --- | --- | --- | --- |
| **Drill ID** | **WebGoat section** | **Module** |  |
|  | Intro | How to work with WebGoat |  |
|  | General | Http Basics |  |
|  | Access Control Flaws | Using an Access Control Matrix |  |
| Access Control Flaws | Bypass a Path Based Access Control Scheme |  |
| Access Control Flaws | LAB: Role Based Access Control  Stage 1: Bypass Business Layer Access Control |  |
| Access Control Flaws | LAB: Role Based Access Control  Stage 3: Bypass Data Layer Access Control |  |
|  | Authentication Flaws | Forgot Password |  |
| Authentication Flaws | Basic Authentication |  |
| Authentication Flaws | Multi Level Login 1 |  |
| Authentication Flaws | Multi Level Login 2 |  |
|  | Parameter Tampering | Bypass HTML Field Restrictions |  |
| Parameter Tampering | Exploit Hidden Fields |  |
|  | Session mgr flaws | Spoof an Authentication Cookie |  |
| Session mgr flaws | Session Fixation |  |
|  |  |  |  |