Intro. to Computer Security: Exercise 4

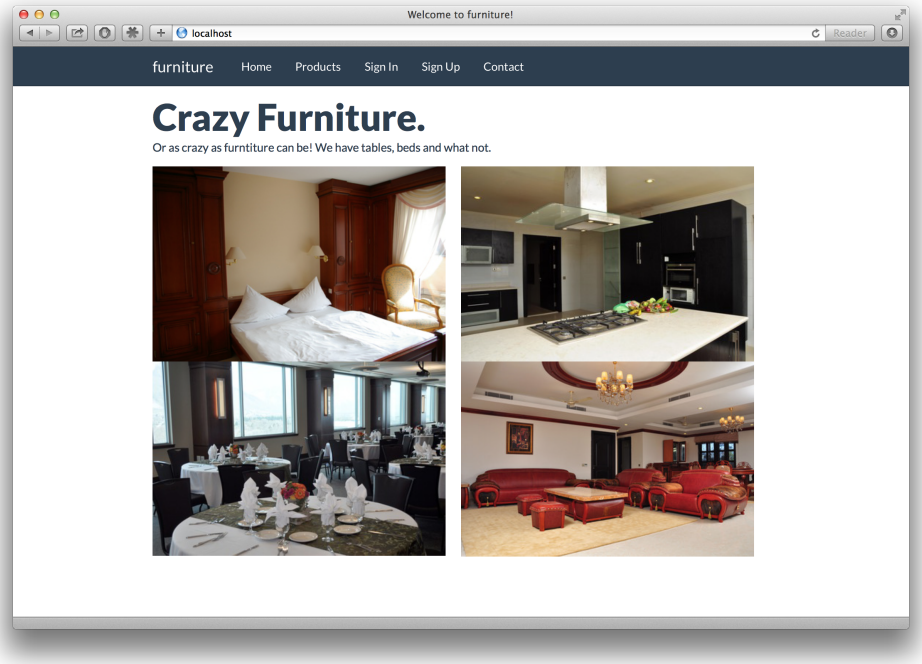
Deadline: 12:00 noon on Friday the 11th of March

Web Security

This exercise looks at web security. The exercise VM has a webserver running on port 80. The source code for this website can be found in the `/var/www/` directory. As you might have guess this website contains many security vulnerabilities.

Connecting to the VM

You can access the website from inside the VM. The `elvis:costello` account contains a copy of the Burp proxy, which you will fine helpful. You can also connect to the VM from your own laptop. See Canvas for details of how to set this up, and see us in the Lab sessions if you need help with this. You will then see this website:



Attacking the website

The website contains a number of different vulnerabilities. Find attacks, which could be carried out by a **remote attacker via the website (i.e. over port 80)**, that would make it possible to:

1. Log in as one of the existing users. **[2 marks]**
2. Get full administrative privileges on the website. **[3 marks]**
3. Find an XSS attack that will let you acquire the admin's session cookie (we want to know where you would attack and how). **[3 marks]**
4. Find a SQL injection attack that will let you view all of the CVVs stored on the site (N.B. we are looking for a single SQL attack that gets the CVVs not logging into each account one by one and viewing them). **[4 marks]**
5. Find a vulnerability in the website that will let you execute any command you want on the web server. **[4 marks]**

For each of these, you must describe how the attack can be performed and the flaw in the application you are exploiting in detail. Please note: the marks are not for finding the attack, rather the marks are for a full and clear description of the vulnerabilities, which demonstrates a complete understanding of the issues. Submit your answers via the Exercise 4 quiz on Canvas.

If you are able to complete all of the above exercises, you might also like to:

- Find a way to view the source files in /var/www.
- Register a new account with a email that isn't on the *bham.ac.uk* domain.
- Describe a CSRF attack that could be used to add something to someones basket (N.B. you can't perform the CSRF unless you create your own website).
- Find an attack that shows you all of the credit card numbers that have been used with this site.
- Implement fixes for the vulnerabilities you found.

There are no marks for these exercises, however doing them will give you a better understanding of how websites work, and fail. If you find the attacks please let me know and/or post to Facebook.

Getting Help

The paper: "The OWASP Top - 2013" (`http://bit.ly/19vuaTV`) provides an excellent description of the kinds of web attacks you can use to complete these exercises. The best place to get direct help is my office hour (Tuesday 11-13).