Security and Networks: Exercise 4

Deadline: 20 April 4pm for Edgbaston Students, 24 April 4pm for Dubai students

Web Security

It's time to take a look at the company's website and find out what is really going on. You can find the company's site by going to 127.0.0.1 on the VM. This address will not work from outside the VM. You can find a copy of the Burp proxy in the Alice account: `aliceBlack:aliceGHdj%*3`. You can also get (and attack) the website by going to 192.168.56.101 (or whatever the IP address of your VM is) on your laptop once the VM is running. The source code for this website can be found in the `/var/www/html` directory. As you might have guessed this website contains many security vulnerabilities.

Attacking the website

This website looks like a furniture store, but you suspect that there is more going on. You need to investigate this site and look for web vulnerabilities. All your attacks must be carried out via the website (i.e. over port 80).

1. **Investigate the products:** Find a SQL injection attack that makes the site display *all* of the products it has in the database. One of the products that is not normally displayed includes a token, submit this token to the token submission website.

   [1 mark]

2. **Get access to the hidden site:** Investigate the websites cookies and find a way to get access to the hidden content on the site using an account you have created on the website yourself. You will find a token displayed on the main page of the hidden site, submit this token.

   [2 marks]

3. **Escalating your privileges:** Find the admin control panel, and from here log into the User Management page. On this page you will find another token, submit this.

   [3 marks]

4. **Get access to the database:** Find a *file upload attack* and use it to upload some php that lets you view the source code of the `mysql.php` page. On this page you will find the sql database password. Use this to access the database where you will find another token. Once you know the password, you can do this from the VM command line with `mysql -h 127.0.0.1 -u <username> -p`. Submit this token to the token submission website. **[4 marks]**

5. **Shell injection:** Find a shell code injection attack on the website and use it to view the file `/webtoken`. Submit this to the token website.

[4 marks]

Getting Help

The paper: "The OWASP Top[1]" 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 the lab session.

[1] `https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project`