Network and Web Security

Additional Web security VM

March 9, 2021

Dr. Tom Chothia and his team at the University of Birmingham have kindly provided this VM for you to further practice the hands-on skills of our course.

The target website runs on a VM that you can download from `https://www.doc.ic.ac.uk/~maffeis/331-vms/ICS_17_v2.ova`. Import the appliance on your VirtualBox like you did for the other tutorials, and connect its network adapter to `dirtylan`. Use your Kali VM to find the "Sensible Furniture" website. It 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). You may find Burp very useful for this exercise.

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 kudo]

2. **Get access to the hidden site:** Investigate the website's 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. *(Hint: remember that if a hash is not "salted" it can be vulnerable to an offline dictionary attack.)*

   [2 kudos]

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

   [3 kudos]

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. Submit this token to the token submission website.

[4 kudos]

5. **Stored XSS:** Find a stored XSS on one of the pages of the website and use it to deliver a payload that will raise an alert "XSS!" when the vulnerable page is visited. There is no token for this exercise.

   [1 kudo]

6. **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. *(Note: reading the token by exploiting the file upload vulnerability of exercise (4) above is not what you are asked here.)*

   [3 kudos]