Cheat Sheet - PCW File Inclusion

Friday, February 5, 2016 6:18 PM

DVWA File Inclusion

This will be a fairly short and quick guide about the File Inclusion vulnerability.

Local File Inclusion (LFI) is a type of vulnerability most often found on websites. It allows an attacker to include a local file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation. This can lead to something as minimal as outputting the contents of the file, but depending on the severity, to list a few it can lead to:

- Code execution on the web server
- Code execution on the client-side such as JavaScript which can lead to other attacks such as cross site scripting (XSS).
- Denial of Service (DoS)
- Data Theft/Manipulation

Preparation:

To follow this guide you will need a copy of Samurai. If you do not have one, or do not know how to set it up, please see this post.

1. **Open Firefox** by clicking the **Firefox Icon** or going to **Applications > Internet > Firefox Web Browser** and **browse to http://dvwa/**.

2. **Go to the DVWA Security** page and **change the Script Security level to low**.

Now we're ready to try out some file inclusion.

The Attack:

1. Go to the File Inclusion page of DVWA and we will get started.

2. Click the View Source button to see what the File Inclusion Source looks like, this will give us an idea of how this works and what we can do.

Now we can see that there is no filtering of what we include, so lets try some things out.

3. Change the URL from **http://dvwa/vulnerabilities/fi/?page=include.php** to **http://dvwa/vulnerabilities/fi/?page=/etc/passwd** and see what happens.

As you can see, we get the contents of the passwd file and a few error messages. We now know the name of every user who can log into the local system, but what about all of the groups that exist?

4. Again change the URL to **http://dvaw/vulnerabilities/fi/?page=/etc/group** and see what happens.

Again, we get the contents of the group file and some error messages. We could view the contents of any file the web server has read access to. If this were a truly insecure website, we could also use this to view pages on other websites by changing the URL like we did before but instead pointing to a remote file or webpage.

From <http://caffeinept.blogspot.com/2012/01/dvwa-file-inclusion.html>