Malicious File Execution

Monday, November 6, 2017 8:48 PM

- Many sites allow the user to upload files, such as images or videos
- Without proper security, files containing malicious commands can be executed on the server

Solution:
The first step of malicious file execution is to create a file that we can run on the server. In this lesson, our goal is to create the file guest.txt in the directory provided in the lesson (the path is generated based on your system).

To do this, we write a .jsp file that uses the java createNewFile() command. The file contents will look like this:
<HTML> <% java.io.File file = new java.io.File("filepath\\guest.txt"); file.createNewFile(); %> </HTML>

The <% indicates that the upcoming code is a java servlet, so java code is allowed. Make sure you fill in the filepath correctly - each directory must be separated by \\, not \. The filename of the .jsp doesn't matter, as long as you know what it is.

Next, we need to figure out where the files are being uploaded so we can execute them. In this case, since we are shown the image, this is very easy. Upload an image using the form, then right click on it and check its properties.

File path for the uploaded image (and our .jsp) in Firefox.

The URL should look something like http://localhost/WebGoat/uploads/image.jpg.
The last step is to upload our malicious .jsp and browse to it so it will execute. Upload the file, then type its address into your browser. The address should be something like http://localhost/WebGoat/uploads/yourfile.jsp.

A blank page will load. You can then return to the lesson and refresh, completing the lesson.