

HACKER VS DEVELOPER...!!

sebelum memulai kita persiapkan dulu alat 2nya

1. localhost (xampp,lampp,appserv,et c) at au web pun boleh
2. notepad
3. buat folder dengan nama "image"

[start of war]

##developer

buat file php

dengan script:

```
<?php
if(isset($_POST['upload'])) {
    $target_path="image/";
    $target_path = $target_path.basename($_FILES['img']['name']);
    if(move_uploaded_file($_FILES['img']['tmp_name'],$target_path)){
        echo "the file " . basename($_FILES['img']['name']) . " has been uploaded! ";
    }else {
        echo "there was an error uploading the file ,please try again!";
    }
}

?>

<form action="" method="post" enctype="multipart/form-data">
<input type="file" size="20" name="img" />
<input type="submit" name="upload" value="Upload" />
```

</form>

lalu simpan di web/localhost tadi

lalu buka filenya di localhost atau web kamu

silahkan upload shell

dan hasilnya pasti bisa

patching 1#

kemudian si developer mempatching script

```
$target_path="image/";  
$target_path=$target_path.basename($_FILES['img']['name']);  
if(move_uploaded_file($_FILES['img']['tmp_name'],$target_path)){  
echo "the file " . basename($_FILES['img']['name']) . " has been uploaded! ";  
}  
else {  
echo "there was an error uploading the file ,please try again!";  
}
```

dengan

script "PHP Arbitrary File"

guna menentukan file apa aja yang bisa masuk melalui file upload tersebut

scriptnya ialah:

```
if($_FILES['img']['type'] != "image/gif") {  
    echo "Sorry, we only allow uploading GIF images";  
    exit;  
}  
  
$uploaddir = 'image/';  
$uploadfile = $uploaddir . basename($_FILES['img']['name']);  
if (move_uploaded_file($_FILES['img']['tmp_name'], $uploadfile)) {  
    echo "File is valid, and was successfully uploaded.\n";  
} else {  
    echo "File uploading failed.\n";  
}
```

sehingga menjadi:

```
<?php  
if($_FILES['img']['type'] != "image/gif") {  
    echo "Sorry, we only allow uploading GIF images";  
    exit;  
}  
  
$uploaddir = 'image/';  
$uploadfile = $uploaddir . basename($_FILES['img']['name']);  
if (move_uploaded_file($_FILES['img']['tmp_name'], $uploadfile)) {  
    echo "File is valid, and was successfully uploaded.\n";  
} else {
```

```

echo "File uploading failed.\n";
}

?>

<form action="" method="post" enctype="multipart/form-data">

<input type="file" size="20" name="img" />

<input type="submit" name="upload" value="Upload" />

</form>

```

melihat hal itu si attacker pun mencari kelemahan script tersebut kemudian si attacker membaca cara kerja dari script tersebut yakni script tersebut akan meloloskan suatu file yang memiliki content-type "image/gif" selain itu gagal terupload dengan informasi tersebut si attacker lalu membuat sebuah teknik yang memerlukan sedikit bantuan addon semisal tamperdata atau yg sejenis

bypass 1#

1. install addon tamperdata di firefox
2. shell.php rename jadi shell.php.jpg atau shell.jpg
3. hidupkan tamperdata: tools -> tamper data -> start tamper
4. upload shell.php.jpg tadi -> klik upload -> lalu tamper
5. kemudian cari nama file "shell.php.jpg" lalu ganti dengan shell.php -> ok

hasil: shell pun terupload

patcing2

melihat script uploadnya bisa di bypass attacker si developer tadi memutar otaknya mencari cara patcingnya akhirnya ia menemukan cara yaitu dengan memanfaatkan system blacklist yakni membatasi

jenis2 file yang sudah di blacklist cara patchingnya adalah dengan cara mengganti script:

```
if($_FILES['img']['type'] != "image/gif") {  
    echo "Sorry, we only allow uploading GIF images";  
    exit;  
}  
  
$uploadaddir = 'image';  
$uploadfile = $uploadaddir . basename($_FILES['img']['name']);  
if (move_uploaded_file($_FILES['img']['tmp_name'], $uploadfile)) {  
    echo "File is valid, and was successfully uploaded.\n";  
} else {  
    echo "File uploading failed.\n";  
}
```

dengan script blacklist:

```
$blacklist = array(".php", ".html", ".shhtml", ".phtml", ".php3", ".php4");  
foreach ($blacklist as $item) {  
    if(preg_match("/$item$/", $_FILES['img']['name'])) {  
        echo "We do not allow uploading PHP files.\n";  
        exit;  
    }  
}  
  
$uploadaddir = 'image';  
$uploadfile = $uploadaddir . basename($_FILES['img']['name']);
```

```

if (move_uploaded_file($_FILES['img']['tmp_name'], $uploadfile)) {
    echo "File is valid, and was successfully uploaded\n";
} else {
    echo "File uploading failed\n";
}

```

sehingga menjadi:

```

<?php
$blacklist = array('.php','.html','.shtml','.phtml', '.php3', '.php4');
foreach ($blacklist as $item) {
    if(preg_match("/$item$/", $_FILES['img']['name'])) {
        echo "We do not allow uploading PHP files\n";
        exit;
    }
}

$uploadaddir = 'image/';
$uploadfile = $uploadaddir . basename($_FILES['img']['name']);
if (move_uploaded_file($_FILES['img']['tmp_name'], $uploadfile)) {
    echo "File is valid, and was successfully uploaded\n";
} else {
    echo "File uploading failed\n";
}

?>

<form action="" method="post" enctype="multipart/form-data">

```

```
<input type="file" size="20" name="img" />
<input type="submit" name="upload" value="Upload" />
</form>
```

dengan script di atas ketika sang attacker mengupload shellnya dengan cara ## bypass 1## maka attacker mendapatkan pesan bahwa file nya tidak bisa terupload.

bypass 2

Dengan kegagalan ini sang attacker pun kembali menganalisa script yang ada di atas dan menyimpulkan bahwa ketika shell di tamper dengan nama shell.php bisa error dikarenakan ekstensi .php telah masuk daftar blacklist sehingga akan menjadi error melihat hasil kesimpulan tersebut si attacker pun mencoba serangan yakni mencoba mengupload dengan ekstensi acak untuk meyakinkan bahwa ini benar2 script blacklist

kali ini si attacker mencoba mengupload dengan ekstensi .f73 (namanya juga acak :v) dan berhasil dengan ini si attacker yakin bahwa script diatas adalah script blacklist dan script blacklist tersebut mempunyai kelemahan dimana dia hanya memblacklist jenis file yang ada pada array jadi ekstensi .php ada dalam daftar array tersebut si attacker pun memulai bypass nya yakni dengan mencoba mengupload dengan ekstensi .php3 .php4 .php5 .PHP .pHp dan lain2

alhasil si attacker pun kembali sukses mengupload shell nya

patching3

tak berhenti disitu persaingan sang develop dan attacker masih berlanjut mengetahui kalau script blacklist nya masih mampu ditembus kemudian sang developer kembali berfikir keras memikirkan bagaimana patchingnya kemudian dia menemukan cara yakni dengan script mime lalu dia mengubah script nya menjadi

```
<?php
$imageinfo = getimagesize($_FILES['img']['tmp_name']);
if($imageinfo['mime'] != 'image/gif' && $imageinfo['mime'] != 'image/jpeg') {
```

```
echo "Sorry, we only accept GIF and JPEG images\n";  
exit;  
}
```

```
$uploadaddir = 'image/';  
$uploadfile = $uploadaddir . basename($_FILES['img']['name']);  
if (move_uploaded_file($_FILES['img']['tmp_name'], $uploadfile)) {  
echo "File is valid, and was successfully uploaded.\n";  
} else {  
echo "File uploading failed.\n";  
}  
>
```

```
<form action="" method="post" enctype="multipart/form-data">  
<input type="file" size="20" name="img" />  
<input type="submit" name="upload" value="Upload" />  
</form>
```

cara kerja script mime ialah dimana dia hanya mengijinkan file yang mempunyai header jpg atau gif
guna meloloskan file agar bisa di upload

dengan ini si attacker pun tak bisa mengupload shellnya walaupun di rename jpg karena tak mempunyai header image

##bypass3##

dengan mengetahui cara kerja tersebut sang attacker pun memulai serangannya

kali ini dia hanya menyisipkan kata

GIF89a;

pada awal script

seperti pada kasus kang hmei7 pada shell J CE (<http://www.joshpate.com/2013/01/how-to-fix-hacked-by-hmei7-on-joomla-web-site/>)

sehingga script menjadi:

```
GIF89a;
```

```
<?php
```

```
script shell
```

```
?>
```

karena sang attacker memanfaatkan comand header (GIF89a;) guna memanipulasi script mime agar mengidentifikasi script shell sebagai image, setelah di rename jadi .gif dan di tamper alhasil sang attacker pun kembali berhasil menembus script mime

```
##patching4##
```

tak tinggal diam ketika sang develop mengetahui script mimenya berhasil ditembus

kemudian dia mulai berfikir keras dan mengumpulkan bahan2 guna meramu script

yang sulit ditembus oleh sang attacker

dan akhirnya dia pun kembali mempatch scriptnya dengan memodifikasinya menjadi:

```
<?php
```

```
if(isset($_POST['upload'])) {
```

```
    $jenis_konten = $_FILES['img']['type'];
```

```

if(preg_match("/image/", $jenis_konten)) {

    $file_sementara = $_FILES['img']['tmp_name'];

    /*
    //periksa lagi, *cacat
    $info_gambar = @getimagesize($file_sementara);

    if(!preg_match("/image/", $info_gambar['mime'])) {
        //belum percaya periksa lagi resolusi *cacat
        if((!isset($info_gambar[0])) && (!isset($info_gambar[1]))) {
            die("Atut, ada hekel... :p");
        }
    }

    $file_dipermanenkan = dirname(__file__)."/".$_FILES['img']['name'];

    if(move_uploaded_file($file_sementara, $file_dipermanenkan)) {
        echo "File <strong>".$_FILES['img']['name']. "</strong> berhasil diunggah.";
    } else {
        echo "Gagal mengunggah!";
    }
}

```

~~*~~

```
$file_dipermanenkan = "" . sha1(rand(0,9999)) . ".jpg";  
$filename = $file_sementara;  
$percent = 1;  
  
// ciplak resolusi  
// pendeteksian ini masih bisa lolos dgn teknik RGB  
$size = getimagesize($filename); //diambil dari file temp, bukan $_FILE['mime']  
$width = $size[0];  
$height = $size[1];  
$mime = $size['mime'];  
  
//jika butuh memperkecil gambar  
$new_width = $width * $percent;  
$new_height = $height * $percent;  
  
// buat gambar baru  
  
if(preg_match('/png|jpeg|jpg|gif/', $mime)) {  
    $image_p = imagecreatetruecolor($new_width, $new_height);  
    if((preg_match('/jpg/', $mime)) || (preg_match('/jpeg/', $mime))) {  
        $image = imagecreatefromjpeg($filename);  
    }  
}
```

```

        if(preg_match('/png/', $mime)) {
            $image = imagecreatefrompng($filename);
        }

        if(preg_match('/gif/', $mime)) {
            $im = imagecreatefromgif($filename);
        }
    }

    if(!@imagecopyresampled($image_p, $image, 0, 0, 0, 0, $new_width, $new_height, $width, $height)) {
        $image_p = imagecreate(200, 100);
        $bg = imagecolorallocate($image_p, 255, 255, 255);
        $black = imagecolorallocate($image_p, 0, 0, 0);
        imagestring($image_p, 5, 2, 2, 'Gambar Korupsi', $black);
    }

    // Output
    imagejpeg($image_p, dirname(__FILE__).'file_dipermanenkan', 100);
    echo '<a href="'. $file_dipermanenkan ."'>.$file_dipermanenkan'</a>';

} else {
    echo "Jenis file yang anda unggah bukan gambar.";
}
}

?>

<form action="" method="post" enctype="multipart/form-data">

```

```
<input type="file" size="20" name="img" required="on" />  
<input type="submit" name="upload" value="Upload" />  
</form>
```

jujur sampai sekarang saya belum bisa nembus script patch yang terakhir diatas heheheh selesailah sampai disini cerita persaingan makhluk dibalik monitor namun dari cerita panjang ini kita pasti akan mendapat banyak pelajaran dan ilmu yang baru heheh sengaja saya buat cerita agar tidak terlalu kaku ketika kita membaca tutorial...

Terimakasih...