

Guía para WarGames

Por: Crack_X: cybersurfer [@] gmail [.] com
<http://foro.elhacker.net/index.php/topic,71763.0.html>

Antes que nada deben considerar que los retos están hechos para pasarse. Siempre va haber una forma de pasarlos y siempre van haber pistas. Las pistas la pueden encontrar en el código fuente de una página , en los headers del http y en los foros. La mayoría de las webs tienen sus foros para ayudar , ahí siempre encuentras muchas pistas y si no las hay pues la pides.

- Los códigos fuente:

Este es el primer lugar por donde empezar a buscar en un reto , al menos que ya sepas por donde va la cosa. Puedes ver el código fuente dando un click derecho->Ver código fuente. En caso de que la pagina tenga deshabilitado los click derecho pues vas a Ver->Código Fuente y si eso tampoco funciona pues pones en el browser "view-source:http://www.google.com" , claro que donde va google pones la web que quieras ver.

Muchas veces dejan mensajes ocultos en los códigos fuentes y son fáciles de distinguir porque empiezan están entre esto "<!-- -->" o lo encuentras porque vez que el código se desajusta en alguna parte , ya que normalmente siguen un patrón por ser auto-generadas (en caso de paginas en php o asp).

- Javascript:

Javascript es conocido como el reto de tontos , porque son los mas fáciles de solucionar aunque hay retos de javascript que son sumamente complicado (solo he visto como 4 de estos). No piensen que van a poder leer todos los retos de javascript por leer estos consejos , la mejor manera de prepararse para estos retos son aprendiendo javascript aunque sea un poco.

Lo primero que tenemos que tomar en cuenta son los inputbox(). Estos que salen como una cajita , te piden una contraseña y luego te redireccionan sin permitirte ver la web. Esto son simples, antes que te salga la cajita le das a "Escape" para que la web se pare. Luego vez el código fuente para ver donde es que sale el inputbox y con que lo compara o que sucede.

A veces te muestran un código falso pero es muy parecido a lo que andas buscando. Esto se debe a que usan un Código:

```
<script src="xxx">
```

, esto significa que el javascript se encuentra en el "src" y el que muestran nunca se ejecuta. Nunca se dejen engañar por el archivo a que señala los "src" , ya que un javascript puede estar en cualquier archivo y no importa la extensión. Y puede darse el caso de que hallan múltiples "src" y solo uno o dos sean verdadero (me ocurrió en hackers). Muchas personas no saben como encontrar esos archivos "ocultos" y lo que hacen es descargar la web entera. Van a Archivo->Guardar como.... , esto lo que hace es descargar todo el código html de la pagina con todos los archivos que tenga linkeado.

Tu mejor amigo siempre va ser alert(). Si tienes un código muy largo que encripta variables y todo eso para generar la comparación , tienes 2 opciones reproducir todo el código y ver lo que hace o añadirle al código alert(variable) para que te diga que contiene la variable. Con alert() es la forma mas simple de ver el valor de una variable. Para añadirle el alert() tienes que reproducir el código o descargar la pagina y agregarle eso al código fuente.

Los un/escape() solo codifican los textos en código url. Lo mas usual es que se hagan muchos unescape() de una variable o c hace queda un poco oculto el código , lo único que tienes que hacer es hacer la función opuesta y poco a poco lo vas a ir sacando el código completo.

Hay un programa llamado htmlock que dice encriptar todo el código de modo seguro pero cada vez que sale una nueva forma pues sale otro tool para desencriptarlo. En un reto de

boinasnegras.com consta de romper esta seguridad y aqui publicaron un mensaje sobre como romper esa seguridad: <http://foro.elhacker.net/index.php/topic,22294.0.html> .

- Http Headers:

Antes que nada deben de leerse el protocolo http , buscando rápido en google encontré esta web que tiene una buena explicación del protocolo "El protocolo Http en Wikipidia" . También pueden buscar el RFC pero creo que esta en ingles solamente. Para ver los headers e información que envían pueden usar el proxomiton y cualquier otro proxy pero mi favorito es el ethereal porque con el puedes observar todas las conexiones que hace tu pc y puedes aprender mucho.

Todo esto te servirá para ver cuando la pagina envía alguna información no visible a los ojos , para que piensen que usas otro navegador o otros OS. Para lo del navegador y el OS muchas personas usan programas que lo editas de modo o facil o pluggins para firefox que hacen esto. Yo prefiero hacerlo por telnet para ver si pasan otra información y en todo caso de que se este haciendo muy complicado pues uso el plugin del firefox. Básicamente en el "User-Agent" es donde esta la información del OS y el navegador , solo tiene que editarlo e ir probando hasta que lo consigan bien.

El Referer sirve para ver de donde proviene una pagina , algunos retos requieren que vengas de una pagina especifica como "fbi.gov" y cosas asi. Pero no solamente sirve para eso , muchas webs tienen un log de los referer y no filtran nada. Si modificamos un referer muchas veces podemos inyectar códigos html , php y asp.

- Exploits:

La mayoría de los wargames sus retos de exploit son bien simple. Constan de un ataque xss , sql injection , remote file inclusión entre otros ataques. También usan software viejos para que busques un exploit viejo y lo uses. Google siempre va ser tu mejor amigo para encontrar esos exploits y a veces tienes que modificarlos un poco , especialmente los de sql injection a un foro o una web. Cambian las tablas y debes modificar el exploit para que te funcione. Lo mejor sobre esto es leer textos sobre estos ataques ya que pueden ir desde un sql injection simple hasta uno complejo.

Algunos textos a leer: A study in Scarlet y los textos de sql injection y otras técnicas que puedes encontrar aqui mismo <http://www.elhacker.net/Textos1.htm> .

Los retos de exploits mas complicados son los de BOF (buffer overflows) y los que requieren estudiar algún software para explotarlo. Pero ambos son pocos comunes en wargames hispanos porque los BOF's son un poco difícil de implementar y muy pocas personas saben como funcionan.

También esta el típico formulario que no permite mas de X caracteres , este solo tienes que reventarlo modificando el tamaño máximo de caracteres o por telnet ya que ahi no los verificara.

En retos para hackear webs las cosas mas comunes a buscar son cookies , directorios , archivos y robots. Algunas webs permiten directory listing , eso es que muestra todos los archivos de una carpeta con tan solo poner www.web.com/directorio/ esto sucede en algunos por defecto al no tener un index. Los robots.txt son archivos que le dan especificaciones a los buscadores , si no quieres que un buscador indexe un fólder o un archivo pues lo veras en el archivo robots.txt . En el muchas veces buscas el archivo o directorio que necesitas para pasar el reto.

Para los archivos , siempre estar pendiente de a que carpetas se le hace referencia en los códigos html. Ya sea una imagen , flash , applet o otra cosa que sea llamada a algún directorio extraño ejemplo:

Código:

```

```

Eso es una pista , significa que hay un directorio llamado secreto y seguro que debes buscar algo por ahí.

- Hashes:

Existen muchos tipos de hashes pero los mas comunes son: md5,md4, sha , rpdm-160, DES , LM y NTLM. Esto son retos fáciles normalmente uno se da cuenta el tipo de hash que es por sus números de bytes o caracteres. El md5 es típico por tener 32 caracteres mientras que el DES es típico por tener caracteres en mayusculas,minusculas y numéricos. Para mi el mejor cracker es el Cain & Abbel ya que permite crackear varios tipos de hashes , luego lo sigue el John The Ripper. Con estos 2 deberían de bastar , en todo caso necesitaras un cracker de algún otro hash especifico.

Un consejo a la hora de crackear un hash. empezar a intentar crackear un hash solamente con números primeros ya que puedes llegar a 8 caracteres numéricos rápido y así sabes si la contraseña es solo numeros. Luego alfanumerico y de por ultimo con todos los caracteres. Ningún hash esta diseñado para ser crackeado con brute-force y que tenga mas de 7 caracteres. En caso de que llegues a 7 caracteres pues empiezas a sospechar y es hora de buscar un diccionario. En el foro se a comentado mucho sobre los diccionarios e incluso hace mucho yo puse un post sobre ellos y me dieron varios enlaces para descargarlos.

Si es un hash poco común como el Crc32 pues tendrás que crear tu propio cracker y aquí entra la ventaja de saber programar en cualquier lenguaje. Para crackers es muy cómodo hacerlos en php ya que php tiene varias funciones para hashes.

- CrackMes:

Este probablemente sea uno de los retos mas difíciles. Lo que mas puede ayudar es la experiencia y leer muchos tutoriales. En el foro hay una muy buena sección de Ingeniería Inversa para dudas y ayuda sobre crackmes. Y en la web y el foro hay muchos tutoriales. Uno de mis tutoriales favorito es Cracker Notas o Notas de un Cracker que da pistas especificas de que buscar en tipos de crackmes pero para esto ya tienes que saber un poco.

Para VB:

Todos sugieren el SmartCheck y claro sus funciones mas buscadas: vbastrcmp, vbavartsteq , vbastrcat , vbastrlen , entre otras.

Para saltar los bugs o trampitas sugiero poner breakpoints en FindWindow y IsDebuggerPresent , este ultimo es el mas usado para saber si están utilizando un debugger.

Y sobre los editores hexadecimales ya eso queda abierto al gusto. Unos prefieren Hackman otros HexWorkShop , esto ya es cuestión del que te sientas mas cómodo.

*****Tutoriales para Ingeniería Inversa*****

<http://foro.elhacker.net/index.php/topic,23911.0.html>

<http://www.elhacker.net/Textos1.htm#cracking>

<http://www.elhacker.net/hacking.htm#crackmes> <-- este para crackmes.

- Crackear Archivos:

Esto es muy parecido a crackear un hash , solo que esta vez es a un archivo. Lo único que necesita es un programa que haga bruteforce al archivo y de estos hay **muchos**. En todo caso que el archivo no se de por vencido vaya intentado con diferentes caracteres (numerico,alfa,alfanumerico,signos) y si aun no cae pues dele con un buen diccionario. Recuerden que el archivo esta hecho para ser crackeado solo es cuestión de paciencia y elegir el buen camino.

-Codigo Fuentes Encriptados

Citar

Solo por ayudar.. una manera mas sencilla de tirar el altrise HTMLock, HTML Protector, AEVITA Strong - Advanced HTML Encrypt ,HTML Guardian, LastBit WebPassword 6.092, Sare2S Webpage Protector, codificacion escape, o url encode (WebMasterScene HTML Protect), y el srcencode de microsoft, y muchos mas sistemas o programas que intentan esconder el codigo fuente.

colocar esto en la barra de direcciones, para ver el codigo fuente escondido (htmllocksrc, HTML protector, etc..)

Code:

Código:

```
javascript:'<xmp>'+document.body.innerHTML
```

y para codificacion con password SOLO EN EL ALTRISE, colocar esto en la barra de direcciones

Code:

Código:

```
javascript:document.write(document.documentElement.innerHTML.split("if(er==1)alert(msg);return%20false;").join(""));document.forms[0].pwd.value="<HTML><TITLE>";document.forms[0].submit.click();document.forms[0].submit.click();
```

Y oprimir el boton de show!!

Para probar dar en los demos de..

<http://www.atrise.com/htmllock/>

http://www.protware.com/demo_e.htm

<http://www.aevita.com/web/lock/samples.htm>

<http://www.share2s.com/web-encrypt.html>

http://www.antssoft.com/htmlprotector/protected_sample.htm

<http://lastbit.com/webpsw/sample3.htm>

Fuente: <http://foro.elhacker.net/index.php/topic,98575.0.html>

Saludos,

Gracias a ElJuAnKaR o FeRmO por recordarme de algunos puntos que no tenia anotados aun. Y gracias Sirdarckcat por crear el pequeño tutorial para mostrar códigos "ocultos".