Solución al Reto Hacking IV de Informática 64

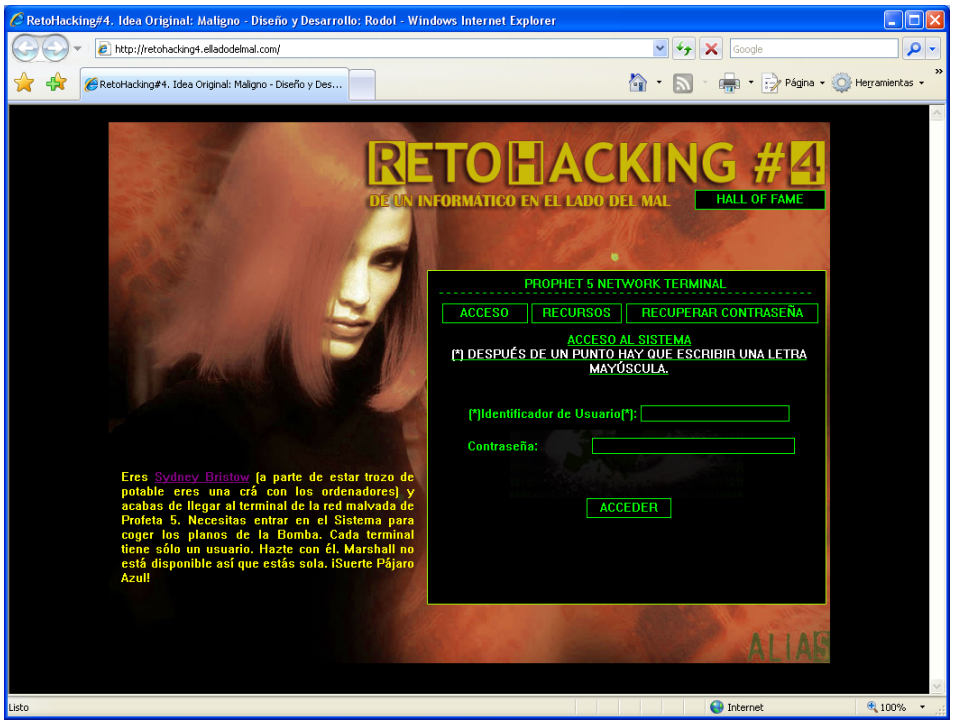
Septiembre 2007 © Daniel Kachakil

Introducción

Este documento describe una posible solución al Reto Hacking IV de Informática 64 que se publicó el 31 de agosto de 2007 en la siguiente dirección web:

http://retohacking4.elladodelmal.com

El reto consistía en conseguir acceso al sistema (usuario y contraseña).



Pistas

En esta ocasión únicamente se nos indica que el reto consta de dos pasos. El texto que aparece en la página principal es el siguiente:

> *Eres Sydney Bristow (a parte de estar trozo de potable eres una crá con los ordenadores) y acabas de llegar al terminal de la red malvada de Profeta 5. Necesitas entrar en el Sistema para coger los planos de la Bomba. Cada terminal tiene sólo un usuario. Hazte con él. Marshall no está disponible así que estás sola. ¡Suerte Pájaro Azul!*

Análisis inicial

Al acceder a la página principal del reto observamos la existencia de cuatro secciones claramente diferenciadas:

- **Acceso:** Formulario de acceso con los típicos campos de identificador de usuario y contraseña.
- **Recursos:** Formulario de búsqueda de recursos de cada planta. Existen dos listas desplegables que permiten filtrar por tipo de recurso (impresoras y terminales) y por planta (primera, segunda y tercera)
- **Recuperar contraseña:** Aparentemente, el típico formulario de recordatorio de contraseña con los campos de identificador de usuario y respuesta secreta.
- **Hall of fame:** Listado de ganadores del reto. No tiene otra utilidad.

A nivel interno, observamos que todo el sitio web está basado en una única página (default.aspx), cuya extensión y estructura nos indica que está desarrollada con ASP.NET, por si pudiera sernos de utilidad. Dicha página modifica su comportamiento dependiendo de los parámetros que recibe.

- **Acceso:**
  - **ACCEDER:** `Default.aspx?usuario=a&password=a`
- **Recursos:**
  - **BUSCAR:** `Default.aspx?recurso=Terminal&planta=Primera+Planta`
- **Recuperar contraseña:**
  - **CHECK:** `Default.aspx?uid=a&rPassword=true`
  - **RECUPERAR:** `Default.aspx?uid=a&respuesta=a`

Primera fase

Tras analizar el código HTML y JavaScript de la página y realizar las primeras pruebas básicas de inyección SQL sin éxito, todo parece indicar que la solución del reto pasa por obtener primero el identificador de algún usuario y después utilizar el recordatorio de la contraseña de alguna forma para finalmente introducir los datos en la página de acceso. Por tanto, parece ser que nos faltará por aprovechar de alguna manera el buscador de recursos para lograr el primer objetivo, ya que parece no tener otro uso.

El buscador de recursos nos muestra únicamente en forma de iconos el número de recursos públicos que están disponibles en cada una de las plantas del edificio.

	Primera planta	**Segunda planta**	**Tercera planta**
Impresoras	3	1	2
Terminales	3	2	1

No hay forma aparente de conseguir que el buscador nos muestre ninguna otra información en forma de texto, por lo que todo apunta a que será necesaria la utilización de técnicas de inyección ciega. Aunque aún no hemos determinado el tipo de inyección, la propia estructura del buscador finalmente nos lleva a suponer que detrás de dicho buscador se encuentra una implementación de la arquitectura **LDAP** (Lightweight Directory Access Protocol), cuyas formas de ataque mediante inyección son conocidas y están documentadas en varios artículos disponibles en la red. Por ejemplo:

http://www.spidynamics.com/whitepapers/LDAPinjection.pdf
http://www.owasp.org/index.php/LDAP_injection

Tras haber comprendido los fundamentos de la arquitectura LDAP, nos centraremos en los operadores y la sintaxis utilizada para realizar filtrados y búsquedas dentro del directorio (RFC1960). Suponiendo que el buscador es vulnerable a inyección LDAP, veamos el número de recursos obtenidos al ejecutar las siguientes búsquedas:

- `Default.aspx?recurso=*&planta=Primera+Planta`
  - Recursos obtenidos: 6
- `Default.aspx?recurso=*&planta=Segunda+Planta`
  - Recursos obtenidos: 3
- `Default.aspx?recurso=*&planta=*`
  - Recursos obtenidos: 12
- `Default.aspx?recurso=*&planta=*)`
  - Recursos obtenidos: 12
- `Default.aspx?recurso=*)&planta=*`
  - Recursos obtenidos: 23

Por el momento, los resultados obtenidos no contradicen la hipótesis inicial de que el buscador es vulnerable a ataques de inyección LDAP, por lo que continuaremos avanzando en esa línea. Observamos que la última búsqueda realizada obtiene más recursos de los 12 que hasta ahora habíamos detectado con los medios normales, por lo que cabe la posibilidad de que el usuario que buscamos se encuentre entre estos 23 recursos. Suponiendo que el operador que se encuentra detrás del parámetro "recurso" del buscador sea un AND, veamos lo que ocurre al probar con esta búsqueda:

- `Default.aspx?recurso=*)(uid=*)`
  - Recursos obtenidos: 1

Todo parece indicar que ya estamos muy cerca de obtener el nombre de usuario, ya que solamente nos falta por determinar el UID probando las letras una a una, utilizando el carácter comodín (el asterisco). Si como resultado obtenemos un recurso, entonces la condición de nuestra búsqueda se debe interpretar como cierta, mientras que si no obtenemos ningún recurso, la condición se interpretará como falsa.

- `Default.aspx?recurso=*)(uid=a*)`
  - Recursos obtenidos: 0
- `Default.aspx?recurso=*)(uid=b*)`
  - Recursos obtenidos: 0
- `Default.aspx?recurso=*)(uid=c*)`
  - Recursos obtenidos: 0
- `Default.aspx?recurso=*)(uid=s*)`
  - Recursos obtenidos: 1

Ya tenemos el primer carácter del usuario (una "s"). Para obtener los siguientes caracteres, podemos continuar de la misma forma, aunque existe otra versión más eficiente y rápida, consistente en utilizar una búsqueda binaria subdividiendo el espacio de caracteres sucesivamente de esta manera:

- `Default.aspx?recurso=*)(uid>=sm)`
  - Recursos obtenidos: 0
- `Default.aspx?recurso=*)(uid>=sf)`
  - Recursos obtenidos: 0
- `Default.aspx?recurso=*)(uid>=sd)`

  - Recursos obtenidos: 1
- `Default.aspx?recurso=*)(uid>=se)`
  - Recursos obtenidos: 0

Ahora que ya tenemos los dos primeros caracteres ("sd"), continuamos con la búsqueda hasta determinar el nombre de usuario completo, sin olvidar que existen otros caracteres usables como los dígitos y los signos de puntuación.

- `Default.aspx?recurso=*)(uid>=sd6.sl)`
  - Recursos obtenidos: 1
- `Default.aspx?recurso=*)(uid>=sd6.sm)`
  - Recursos obtenidos: 0

Finalmente obtenemos los 16 caracteres del nombre de usuario y pasamos a la siguiente fase. Como se puede apreciar a posteriori, evidentemente era imposible conseguir el nombre utilizando ataques de fuerza bruta o de diccionario.

Segunda fase

Ahora que ya tenemos el nombre de usuario, probamos a introducirlo en el formulario de recuperación de contraseña para ver lo que ocurre y obtenemos la siguiente pregunta secreta:

¿Dónde se cerró el Círculo?

Tras descartar posibles vulnerabilidades en el sistema de recuperación de contraseñas y ante la imposibilidad de encontrar la forma de obtener la contraseña mediante inyección LDAP o usando otras técnicas, todo apunta a que esta fase es tan simple como aparenta. Parece ser que solo hay que acertar la respuesta a la pregunta.

Tampoco es de extrañar que esta sea la forma de superar esta fase, ya que en la vida real nos encontramos con este mecanismo de recordatorio de contraseñas en muchos sitios web (¿acaso nunca lo has intentado con alguna cuenta de Hotmail?) ;-)

Al final deducimos que la respuesta debe estar relacionada con la serie Alias que ambienta la página del reto y utilizamos el buscador que más nos guste con el fin de encontrar páginas relacionadas con esa serie televisiva y que nos detalle al máximo el argumento de cada capítulo, centrándonos en encontrar la palabra "círculo".

En mi caso, esta fase me costó mucho más que la primera porque ya no sabía lo que probar (sí, ya sé que no he sido el único), pero finalmente obtuve la respuesta con un poco de ayuda de un amigo que conocía a otro que sí había visto la serie que me pasó un link que acotaba un poco más la interminable búsqueda entre los 105 capítulos de la serie). Buscando en Google los términos *"prophet five circle completed"* (sin comillas) encontrábamos como primer resultado esta página en la que se encuentra la solución a la pregunta (dos palabras de 3 y 6 letras):

http://www.neloo.com/alias/about7.html

Una vez introducida la respuesta a la pregunta, obtenemos la contraseña del usuario (de nada menos que 28 caracteres, por cierto) e introducimos estos datos en el formulario de acceso de la página principal, lo que nos lleva a completar el reto y a encontrarnos con una pequeña sorpresa a la hora de introducir nuestro nombre (mejor si lo hacemos con los altavoces encendidos)

Agradecimientos

Como siempre, quiero terminar agradeciéndote la lectura de este documento, esperando que te haya resultado didáctico, aunque no sin antes reconocer y agradecer el esfuerzo de los creadores de este reto, Chema y Rodol, porque montar estas cosas cuesta más tiempo de lo que parece. Y por qué no, también le agradezco a Pedro Laguna que se fuera a cenar por ahí aquél sábado en el que obtuve el tercer puesto, ya que me consta que había conseguido el nombre de usuario antes que yo ;-)

Saludos,

Daniel Kachakil
dani@kachakil.com