Proyecto Final del Curso 2

Manual de Usuario

Nombre del Proyecto

Escaneo Web

Objetivo del Proyecto

Creación de herramienta para escaneo Web.

Descripción del proyecto

Creación de una herramienta que permita obtener información de sitios Web, que hagan uso de gestores de contenido Moodle.

Herramienta 1

Web crawling y divulgación de información.

Integrantes del equipo de desarrollo

Mario Arturo Pérez Rangel
José Luis Torres Rodríguez

Manual de Usuario

moodlecrawl es una herramienta que implementa un 'web crawling' para sitios basados en Moodle, lleva a cabo un análisis del sitio indicado revisando la información divulgada por el servidor Web. Realiza un análisis de las principales cabeceras devueltas por el servidor Web para las peticiones HTTP, llevando a cabo un diagnóstico y mostrando recomendaciones para aquellas que pueden representar problemas de seguridad.

Forma de uso de la herramienta:

```
moodlecrawl [--help|-h] [[--ip|-s] <direccion ip>] [[--dic|-d]
<diccionario>] [[--login|-l] <usuario>] [[--pass|-p] <password>]
[[--report|-r] [text|html]] --url URL
```

Donde:

`--help o -h`	Muestra la ayuda
`--ip o -s`	Indica la dirección IP del equipo a analizar
`--dic o -d`	Indica el nombre del archivo que contiene el diccionario de directorios a revisar en el equipo a analizar.
`--login o -l`	Indica el nombre de usuario a usar para conectarse al equipo analizado.
`--pass o -p`	Indica el password a utilizar para conectarse al equipo analizado.
`--report o -r`	Indica cómo se debe generar el reporte. Las opciones son 'text' y 'html', siendo la primera la opción predeterminada.
`--url`	Se utiliza para introducir la URL a analizar

Las opciones **`--ip`** y **`-s`** son excluyentes con la URL. En caso de incluirse una de las opciones y la URL, esta última se ignorará y se hará uso de la expresión incluida en las opciones mencionadas. Todos los parámetros son opcionales.

Ejemplos de uso:

El siguiente comando realizará un análisis del sitio indicado, mostrando los resultados en formato de texto, directamente en la terminal:

```
$ moodlecrawl --url https://aula.cert.unam.mx/
```

```
Analisis de encabezados:

Cabecera Server:
        Valor devuelto: Apache
        Diagnostico: ServerTokens configurados.

Cabecera X-Powered-By
        Diagnostico: Cabecera X-Powered-By deshabilitada.

Cabecera X-XSS-Protection:
        Diagnostico: X-XSS-Protection no esta habilitada.
        Recomendacion: habilitar el encabezado 'X-XSS-Protection:
1;mode=block' para reducir el riesgo de ataques de tipo XSS.

Cabecera X-Frame-Options:
        Valor devuelto: SAMEORIGIN, sameorigin
        Diagnostico: X-Frame-Options esta habilitada.

Datos del servidor:
        Direccion: 132.247.70.140
        Puerto: 443

Cabecera Accept-Ranges:
        Diagnostico: Accept-Ranges deshabilitada, el servidor no
acepta peticiones parciales.
```

Por razones de espacio solamente se incluye parte de la salida, el resto muestra información sobre los errores 403, 404 y 500, además de los directorios descubiertos en el servidor.
De manera predeterminada la herramienta genera un archivo en formato de texto, si se requiere que la salida se genere en formato html se debe agregar la opción **'-r html'**, como se muestra a continuación:

```
$ moodlecrawl --url https://aula.cert.unam.mx/ -r html
```

Esto creará un archivo de nombre moodleCrawlOUT.html con la información del sitio analizado, el cual deberá ser abierto con un navegador Web.

Si se desea hacer uso de un diccionario en particular, el nombre de éste se debe indicar mediante la opción **--dic** ó **-d**. Por ejemplo:

```
$ moodlecrawl --url https://aula.cert.unam.mx/ -r html -d
dicMoodle.txt
```

Si se desea proporcionar las credenciales de un usuario para poder realizar la conexión con el servidor a analizar, éstas se deben incluir con las opciones **--login o -l**, por ejemplo:

```
$ moodlecrawl --url https://aula.cert.unam.mx/ -r html -d
dicMoodle.txt -l usuario1 -p secreto
```

Ésta última instrucción permite analizar la url indicada, haciendo uso del diccionario **`dicMoodle.txt`**, con el nombre de usuario **`usuario1`** y el password **`secreto`**. El reporte se generará en formato html.

Con la opción **`--help`** ó **`-h`** se puede obtener la ayuda de la aplicación, como se muestra en el siguiente ejemplo:

```
$ moodlecrawl --help

metacpan.pl implementa un 'web crawling' para sitios basados en
Moodle, lleva a cabo un analisis del sitio indicado revisando la
informacion divulgada.

Forma de uso:
  metacpan.pl [--help|-h] [[--ip|-s] <direccion ip>] [[--dict|-d]
<diccionario>]
           [[--login|-l] <usuario>] [[--password|-p] <password>]
[[--report|-r] [text|html]] --url URL

Donde:
--help o -h      Muestra esta ayuda
--ip o -s        Indica la direccion IP del equipo a analizar
--dict o -d     Indica el nombre del archivo que contiene el
diccionario de directorios a revisar en el equipo a analizar
--login o -l     Indica el nombre de usuario a usar para conectarse
al equipo analizado
--password o -p  Indica el password a utilizar para conectarse al
equipo analizado
--report o -r    Indica como se debe generar el reporte. Las opciones
son 'text' y 'html', siendo la primera la opcion predeterminada.
--url            La URL del directorio base de moodle.

Las opciones --ip y -s son excluyentes con la URL. En caso de
incluirse una de las opciones y la URL, esta ultima se ignorara y se
hara uso de la expresion incluida en las opciones mencionadas.
Todos los parametros son opcionales.
```

Finalmente, con las opciones **`--ip`** o **`-s`** se puede indicar la dirección IP a analizar.