

# Caso T9

1) En el directorio LDAP de una empresa encontramos las siguientes entradas:

```
dn: cn=u999999a,dc=empresa,dc=es
cn: u999999a
objectClass: inetOrgPersonExtended
objectClass: inetOrgPerson
uid: u999999a
givenName: Antonio
sn: Apellidos de Prueba
nif: 43012345X
memberOf: cn=CONTABILIDAD,dc=empresa,dc=es
memberOf: cn=AUDITORES,dc=empresa,dc=es
mail: toni@empresa.es
mail: adeprueba@empresa.es
mail: antonio.a.p@contabilidad.empresa.es
```

```
dn: cn=u999999b,dc=empresa,dc=es
cn: u999999b
objectClass: inetOrgPersonExtended
objectClass: inetOrgPerson
uid: u999999b
givenName: María
sn: Test Primero
nif: 43092345Z
memberOf: cn=CONTABILIDAD,dc=empresa,dc=es
memberOf: cn=DIRECTIVA,dc=empresa,dc=es
memberOf: cn=INTERNET,dc=empresa,dc=es
mail: maria@empresa.es
mail: mtest@empresa.es
```

```
dn: cn=AUDITORES,dc=empresa,dc=es
cn: AUDITORES
objectClass: groupOfNames
member: cn=u999999a,dc=empresa,dc=es
description: Auditores certificados
```

```
dn: cn=INTERNET,dc=empresa,dc=es
cn: INTERNET
objectClass: groupOfNames
member: cn=u999999b,dc=empresa,dc=es
description: Acceso a Internet
```

```
dn: cn=CONTABILIDAD,dc=empresa,dc=es
cn: CONTABILIDAD
objectClass: groupOfNames
member: cn=u999999a,dc=empresa,dc=es
member: cn=u999999b,dc=empresa,dc=es
description: Departamento de Contabilidad
```

```
dn: cn=DIRECTIVA,dc=empresa,dc=es
cn: DIRECTIVA
objectClass: groupOfNames
member: cn=u999999b,dc=empresa,dc=es
description: Miembros de la directiva
```

```
dn: cn=ACCESO_TOTAL,dc=empresa,dc=es
cn: ACCESO_TOTAL
objectClass: groupOfNames
member: cn=u999999b,dc=empresa,dc=es
description: Acceso total a los sistemas de información
```

Responder a las siguientes preguntas:

a) ¿Qué resultados (especificar el cn solamente) devolverá una query con el siguiente filtro LDAP? (Valor: 5%)

```
(memberOf=cn=INTERNET,dc=empresa,dc=es)
```

b) ¿Qué resultados (especificar el cn solamente) devolverá una query con el siguiente filtro LDAP? (Valor: 5%)

```
(&(memberOf=cn=CONTABILIDAD,dc=empresa,dc=es)(memberOf=cn=DIRECTIVA,dc=empresa,dc=es))
```

c) ¿Qué resultados (especificar el cn solamente) devolverá una query con el siguiente filtro LDAP? (Valor: 5%)

```
(|(givenName=María)(memberOf=cn=ACCESO_BASIC0,dc=empresa,dc=es))
```

d) ¿Qué resultados (especificar el cn solamente) devolverá una query con el siguiente filtro LDAP? (Valor: 5%)

```
(nif=430*)
```

e) ¿Qué resultados (especificar el cn solamente) devolverá una query con el siguiente filtro LDAP? (Valor: 5%)

```
(!(objectClass=groupOfNames))
```

f) Escribir una query que devuelva todos los usuarios del departamento de contabilidad. (Valor: 7,5%)

g) Escribir una query que devuelva todos los usuarios que tengan una dirección de correo que termine en ".es" o ".com". (Valor: 7,5%)

h) Escribir una query que devuelva todos los usuarios cuyo nombre contenga una "s", su apellido empiece por "A" y que no sean miembros de la directiva. (Valor: 7,5%)

i) Escribir una query que devuelva todos los usuarios que no tengan dirección de correo. (Valor: 7,5%)

Valor de la pregunta: 50% de la nota del caso

2) Identificar razonadamente qué problemas de seguridad se producen en el desarrollo de aplicaciones web en cada uno de los siguientes supuestos:

a) La aplicación web permite el acceso al área de administrador introduciendo un PIN de 8 dígitos, cada uno en un recuadro en la pantalla. A medida que se van tecleando dígitos, se van rellenando los recuadros de la pantalla con un asterisco. Una vez se ha introducido el octavo dígito, se envía el PIN al servidor para que lo compruebe. Si este es correcto, se permite el acceso; si no, el servidor espera 10 segundos y devuelve al usuario a la pantalla de introducción del PIN, vaciando los recuadros de los dígitos a partir del primer dígito incorrecto y dejando los anteriores con los valores que había tecleado el usuario (mostrando en pantalla un asterisco, como antes), de manera que se pueda continuar introduciendo el PIN a partir del punto donde se cometió el error. (Valor: 7,5%)

b) La aplicación tiene un control de acceso por usuario y contraseña. Para no tener las contraseñas en texto claro guardadas en el servidor, el programador ha decidido guardar un hash de las mismas. Como el software que utiliza no contiene librerías para el cálculo de hashes, decide definir su propia función de hash de esta manera:

```
hash(S)= base64((XOR de todos los bytes de la cadena S)*38470771)
```

(Valor: 7,5%)

c) Una aplicación utiliza para la autenticación de sus usuarios una librería que almacena las contraseñas aplicándoles un hash SHA-512, para máxima seguridad. En el proceso de autenticación, si un usuario existe, pero la contraseña que ha introducido es incorrecta, se muestra una pantalla estándar de error de la aplicación, que contiene el mensaje "Contraseña incorrecta" y una serie de códigos de diagnóstico para el programador. Entre los datos que figuran en los códigos de diagnóstico, se incluyen la fecha y hora de la petición, el *user agent* del navegador, la versión del servidor de aplicaciones, la ubicación de la instrucción que ha producido el error y los parámetros de las llamadas de función que estaban en la pila en ese momento, que en este caso contienen el hash SHA-512 de la contraseña incorrecta que el usuario ha introducido y el hash SHA-512 de la contraseña correcta almacenada. (Valor: 7,5%)

d) Disponemos de una aplicación para consulta de datos tributarios de los ciudadanos. Como los ciudadanos no disponen de usuario y contraseña, para autenticarlos se les solicita en un formulario el número de NIF, la fecha de nacimiento, el código postal y el valor de una casilla de su última declaración de la renta. El servidor recibe los datos tal como los ha introducido el usuario y, para validarlos, realiza una consulta contra un servidor LDAP que contiene la información necesaria. La consulta se construye a partir de la cadena:

```
(&(nif=$NIF)(fechaNacimiento=$FECHANACIMIENTO)(cp=$CODPOSTAL)(casilla=$CASILLA))
```

En ella se sustituyen los nombres de las variables ("VARIABLE") por el valor de los campos correspondientes. Si el resultado de esta consulta es un solo objeto y el valor de su atributo "nif" es igual al de la variable \$NIF, se permite el acceso. (Valor: 7,5%)

e) Una aplicación de gestión de documentos que se ejecuta sobre un servidor de tipo Linux permite a los usuarios especificar en qué disco se van a guardar los documentos. Para ello, en la pantalla de subida de documentos se incluye una lista desplegable que permite seleccionar una de 3 posibles etiquetas de disco: "solicitudes", "informes" o "resoluciones". El servidor recibe el valor del campo y, para mostrar al usuario el espacio disponible en el disco, ejecuta la llamada estándar del lenguaje C "system", que recibe como parámetro una cadena que contiene la instrucción que se le va a pasar al shell (/bin/bash) para ejecutar. En este caso, se utiliza el siguiente parámetro:

```
/usr/bin/df /dev/disk/by-label/$ETIQUETA >$RESULTADO
```

Donde la variable "\$ETIQUETA" se sustituye previamente a la llamada por el valor de etiqueta de disco recibido y \$RESULTADO por el nombre de un fichero temporal. Una vez ejecutada la instrucción, se lee el fichero temporal con el resultado y de ahí se extrae el valor del espacio libre en el disco que se mostrará al usuario. (Valor: 10%)

f) Una aplicación de consulta de historiales médicos que se ejecuta en un servidor tipo Linux permite a los ciudadanos, entre otras cosas, obtener una copia en PDF de su historial. Dado el carácter especialmente sensible de los datos médicos, se exige a los ciudadanos un certificado electrónico emitido por una autoridad certificadora reconocida para identificarse y se comprueba estrictamente que solo se accede a los datos relativos

al titular del certificado. Para obtener la copia de su historial médico, el ciudadano, una vez identificado, debe seleccionar la opción correspondiente y a continuación pulsar un botón para confirmar la solicitud. La confirmación se solicita debido a que recopilar toda la información del paciente es un proceso potencialmente largo que puede durar desde unos pocos segundos (cuando casi no hay información) hasta varios minutos (cuando hay mucha información). El servidor va recorriendo las distintas tablas de la base de datos y, con la información obtenida, va construyendo un fichero PDF situado en "/tmp/historial.pdf". Cuando ha terminado el proceso, devuelve el contenido del fichero al usuario para que lo guarde o lo visualice. (Valor: 10%)

*Valor de la pregunta: 50% de la nota del caso*