

# Cas T9

1) En el directori LDAP d'una empresa trobam les següents entrades:

```
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: Auditors certificats

dn: cn=INTERNET,dc=empresa,dc=es
cn: INTERNET
objectClass: groupOfNames
member: cn=u999999b,dc=empresa,dc=es
description: Accés 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: Departament de Comptabilitat

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

dn: cn=ACCESO_TOTAL,dc=empresa,dc=es
cn: ACCESO_TOTAL
objectClass: groupOfNames
member: cn=u999999b,dc=empresa,dc=es
description: Accés total als sistemes d'informació
```

Respondre a les següents preguntes:

a) Quins resultats (especificar el cn només) tornarà una query amb el següent filtre LDAP?  
(Valor: 5%)

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

b) Quins resultats (especificar el cn només) tornarà una query amb el següent filtre LDAP?  
(Valor: 5%)

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

c) Quins resultats (especificar el cn només) tornarà una query amb el següent filtre LDAP?  
(Valor: 5%)

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

d) Quins resultats (especificar el cn només) tornarà una query amb el següent filtre LDAP?  
(Valor: 5%)

`(nif=430*)`

e) Quins resultats (especificar el cn només) tornarà una query amb el següent filtre LDAP?  
(Valor: 5%)

`(!(objectClass=groupOfNames))`

f) Escriure una query que torni tots els usuaris del departament de comptabilitat. (Valor: 7,5%)

g) Escriure una query que torni tots els usuaris que tinguin una adreça de correu que acabi en ".es" o ".com". (Valor: 7,5%)

h) Escriure una query que torni tots els usuaris el nom dels quals contingui una "s", el seu cognom comenci per "A" i que no siguin membres de la directiva. (Valor: 7,5%)

i) Escriure una query que torni tots els usuaris que no tinguin adreça de correu. (Valor: 7,5%)

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

2) Identificar raonadament quins problemes de seguretat es produeixen en el desenvolupament d'aplicacions web en cada un dels següents supòsits:

a) L'aplicació web permet l'accés a l'àrea d'administrador introduint un PIN de 8 dígits, cada un en un requadre a la pantalla. A mesura que es van teclejant dígits, es van omplint els requadres de la pantalla amb un asterisc. Una vegada s'ha introduït el vuitè dígit, s'envia el PIN al servidor perquè el comprovi. Si aquest és correcte, es permet l'accés; si no, el servidor espera 10 segons i torna l'usuari a la pantalla d'introducció del PIN, buidant els requadres dels dígits a partir del primer dígit incorrecte i deixant els anteriors amb els valors que havia teclejat l'usuari (mostrant en pantalla un asterisc, com abans), de manera que es pugui continuar introduint el PIN a partir del punt on es va cometre l'error. (Valor: 7,5%)

b) L'aplicació té un control d'accés per usuari i contrasenya. Per no tenir les contrasenyes en text clar guardades al servidor, el programador ha decidit guardar un hash de les mateixes. Com que el programari que utilitza no conté llibreries per al càlcul de hashes, decideix definir la seva pròpia funció de hash d'aquesta manera:

```
hash(S)= base64((XOR de tots els bytes de la cadena S)*38470771)
```

(Valor: 7,5%)

c) Una aplicació utilitza per a l'autenticació dels seus usuaris una llibreria que emmagatzema les contrasenyes aplicant-los un hash SHA-512, per a màxima seguretat. En el procés d'autenticació, si un usuari existeix, però la contrasenya que ha introduït és incorrecta, es mostra una pantalla estàndard d'error de l'aplicació, que conté el missatge "Contrasenya incorrecta" i una sèrie de codis de diagnòstic per al programador. Entre les dades que figuren en els codis de diagnòstic, s'inclouen la data i hora de la petició, el *user agent* del navegador, la versió del servidor d'aplicacions, la ubicació de la instrucció que ha produït l'error i els paràmetres de les cridades de funció que estaven a la pila en aquell moment, que en aquest cas contenen el hash SHA-512 de la contrasenya incorrecta que l'usuari ha introduït i el hash SHA-512 de la contrasenya correcta emmagatzemada. (Valor: 7,5%)

d) Disposam d'una aplicació per a consulta de dades tributàries dels ciutadans. Com que els ciutadans no disposen d'usuari i contrasenya, per autenticar-los se'ls sol·licita en un formulari el nombre de NIF, la data de naixement, el codi postal i el valor d'una casella de la seva darrera declaració de la renda. El servidor rep les dades tal com les ha introduït l'usuari i, per validar-les, realitza una consulta contra un servidor LDAP que conté la informació necessària. La consulta es construeix a partir de la cadena:

```
(&(nif=$NIF)(dataNaixement=$DATANAIXEMENT)(cp=$CODPOSTAL)(casella=$CASELLA))
```

En ella se substitueixen els noms de les variables ("VARIABLE") pel valor dels camps corresponents. Si el resultat d'aquesta consulta és un sol objecte i el valor del seu atribut "nif" és igual al de la variable \$NIF, es permet l'accés. (Valor: 7,5%)

e) Una aplicació de gestió de documents que s'executa sobre un servidor de tipus Linux permet als usuaris especificar a quin disc es guardaran els documents. Per a això, a la pantalla de pujada de documents s'inclou una llista desplegable que permet seleccionar una de 3 possibles etiquetes de disc: "sol·licituds", "informes" o "resolucions". El servidor rep el valor del camp i, per mostrar a l'usuari l'espai disponible al disc, executa la cridada estàndard del llenguatge C "system", que rep com a paràmetre una cadena que conté la instrucció que se li passarà al shell (/bin/bash) per executar. En aquest cas, s'utilitza el següent paràmetre:

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

On la variable "\$ETIQUETA" se substitueix prèviament a la cridada pel valor d'etiqueta de disc rebut i \$RESULTAT pel nom d'un fitxer temporal. Una vegada executada la instrucció, es llegeix el fitxer temporal amb el resultat i d'allà s'extreu el valor de l'espai lliure al disc que es mostrarà a l'usuari. (Valor: 10%)

f) Una aplicació de consulta d'historials mèdics que s'executa en un servidor tipus Linux permet als ciutadans, entre altres coses, obtenir una còpia en PDF del seu historial. Atès el caràcter especialment sensible de les dades mèdiques, s'exigeix als ciutadans un certificat electrònic emès per una autoritat certificadora reconeguda per identificar-se i es comprova estrictament que només s'accedeix a les dades relatives al titular del certificat. Per obtenir la còpia del seu historial mèdic, el ciutadà, una vegada identificat, ha de

seleccionar l'opció corresponent i a continuació prémer un botó per confirmar la sol·licitud. La confirmació se sol·licita pel fet que recopilar tota la informació del pacient és un procés potencialment llarg que pot durar des d'uns quants segons (quan gairebé no hi ha informació) fins a uns quants de minuts (quan hi ha molta informació). El servidor va recorrent les diferents taules de la base de dades i, amb la informació obtinguda, va construint un fitxer PDF situat a "/tmp/historial.pdf". Quan ha acabat el procés, torna el contingut del fitxer a l'usuari perquè el guardi o el visualitzi. (Valor: 10%)

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