Cas S9

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
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=CONTABILIDAD,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=INTERNET,dc=empresa,dc=es))
```

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

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

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

```
(mail=*@contabilidad.empresa.es)
```

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 amb permís d'accés a Internet. *(Valor: 7,5%)*

g) Escriure una query que torni tots els usuaris el primer cognom dels quals comenci per "A" o "B". *(Valor: 7,5%)*

h) Escriure una query que torni tots els usuaris el NIF dels quals acabi en "Z" i que siguin membres de la directiva. *(Valor: 7,5%)*

i) Escriure una query que torni tots els grups que no estiguin buits. *(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 rep un paràmetre a l'URL (per exemple, "http://servidor.dominio.es/BorrarArticulo?id=450") i executa un "DELETE FROM articulos WHERE articulo_id="+id (el paràmetre *id* es rep directament en la variable de tipus cadena denominada *id* i el signe "+" representa en aquest cas la concatenació de cadenes). *(Valor: 7,5%)*

b) L'aplicació conté un carretó de comprar en un formulari amb codi JavaScript que s'encarrega d'omplir els preus dels articles i de realitzar la suma dels mateixos per obtenir l'import total de la comanda. Després, el codi JavaScript fa una cridada a un servei web, passant-li com a paràmetre l'import total i el nombre de targeta del client (més el nom, data de caducitat i altres dades requerides per al pagament). Aquest servei web executa el càrrec de l'import rebut a la targeta de crèdit i, si el banc respon que l'operació ha estat correcta, genera la comanda perquè es processi. *(Valor: 7,5%)*

c) Una aplicació sol·licita a l'usuari un nom d'usuari i contrasenya per permetre l'accés. Amb aquestes dades, la pàgina web genera un autenticador que consisteix en el nom d'usuari i la contrasenya concatenats, que s'envia al servidor. El servidor carrega en una variable de tipus cadena un fitxer de text complet (amb totes les seves línies, incloent els codis de final de línia que les delimiten) en el que en cada línia hi ha un autenticador (usuari concatenat amb la seva contrasenya) autoritzat. Per comprovar que l'usuari està autoritzat, es comprova si l'autenticador rebut apareix en qualsevol posició de la variable

de tipus cadena en la qual s'ha carregat el fitxer d'autoritzacions. Si és així, s'autoritza l'accés. *(Valor: 7,5%)*

d) Una aplicació sol·licita en un formulari un usuari i contrasenya. Per continuar amb la comprovació d'accés, el botó "enviar" del formulari HTML carrega (operació GET) al navegador la següent pàgina, que serà "https://servidor.dominio.es/aplicacion.jsp?usu=USUARIO&pass=CONTRASENYA", on USUARI i CONTRASENYA són els valors que s'han introduït al formulari. El servidor comprova una taula que conté els usuaris i un hash SHA-256 de la contrasenya per comprovar que el hash SHA-256 de la contrasenya rebuda coincideix amb el que està assignat a l'usuari a la taula d'autoritzacions. *(Valor: 7,5%)*

e) Una aplicació de gestió d'historials mèdics identifica un usuari amb certificat digital. Una vegada identificat l'usuari, quan vol consultar un historial d'un pacient, l'aplicació només li mostra aquells per als quals està autoritzat. Quan l'usuari fa clic sobre l'historial que desitja consultar, s'envia al servidor una petició https amb el nombre d'historial com a paràmetre. Com que l'usuari ja està autenticat i només ha pogut escollir entre els historials als que està autoritzat, el servidor, en rebre la petició, torna l'historial especificat comprovant només que existeixi a la base de dades. Els nombres d'historial són enters que el servidor ha anat assignant seqüencialment a partir de l'1 des que va començar a funcionar l'aplicació. *(Valor: 10%)*

f) Una aplicació de consulta de documents situada en un servidor de tipus Linux executa el servidor d'aplicacions amb permisos de "root" i emmagatzema els documents al servidor en fitxers amb el camí "/app/documentos/ANY/MES/DIA/ID", on ANY és l'any de 4 xifres, MES és el nombre del mes, DIA és el nombre del dia i ID és un identificador alfanumèric de 32 caràcters generat aleatòriament per seguretat. Quan es vol descarregar un document, l'aplicació redirigeix a la pàgina "https://servidor.dominio.es/getDocument?path=ANY/MES/DIA/ID". El servidor llavors concatena la cadena "/app/documents/" amb el paràmetre "path" i torna el contingut del fitxer situat en aquesta ubicació al client. Segons els requeriments funcionals, tots els usuaris autenticats han de tenir accés de lectura a tots els documents, per la qual cosa no existeix la possibilitat de comprovar que un usuari tingui permisos per accedir a un document concret. L'aplicació autentica correctament els usuaris, però el servei "getDocument" no comprova l'autenticació, ja que és necessari tenir l'ID correcte per accedir al document i aquesta informació només la poden tenir els usuaris que s'han autenticat correctament en el sistema. *(Valor: 10%)*

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