Er dit login-system sikkert?

Artiklen omhandler en ret banal fejl, der dog kan give store problemer.

Skrevet den **06. Feb 2009** af **netro** I kategorien **Programmering / ASP** | ★☆☆☆☆

Når man laver et login-system på en hjemmeside, er det påkrævet at sætte sikkerheden i højsædet. Mange nybegyndere tror fejlagtigt, at deres system er umuligt at bryde. Dog glemmer de oftest en enkelt lille ting, hvilket denne artikel handler om.
Lad os til at starte med betragte et meget simpelt login-system baseret på en Access-database.

```
<%
Set Conn = Server.CreateObject("ADODB.Connection")
Conn.Open("Driver={MicroSoft Access Driver (*.mdb)};DBQ=" &
Server.MapPath("database.mdb"))

If Request.ServerVariables("Request_Method") = "POST" Then

   Brugernavn = Request.Form("brugernavn")
   Password = Request.Form("password")

   SQL = "Select From Tabel Where Brugernavn = '" & Brugernavn & "' And
Password = '" & Password & "'"
   Set rs = Conn.Execute(SQL)

   If Not rs.EOF Then
      'Brugeren er godkendt
   Else
      'Brugeren er afvist
   End If
End If
%>

<form method="post" action="side.asp">
   <input type="text" name="brugernavn"><br>
   <input type="password" name="password"><br>
   <input type="submit" value="Log ind">
</form>
```

Grundet et alvorligt sikkerhedshul i ovenstående kode, er det muligt at foretage et såkaldt SQL-attack og logge på som den første bruger, der findes i tabellen uden at kende vedkommendes password.
Ønskes dette, gøres det ganske enkelt ved at indtaste følgende i password-feltet.

```
' Or 1='1
```

Og hvad skulle det så bevirke, spørger du muligvis dig selv. Jo, når ovenstående indsættes i SQL-sætningen, manipuleres der faktisk med denne, så forespørgslen til databasen nu ser ud som følger.

```
SQL = "Select * From Tabel Where Brugernavn = '' And Password = '' Or 1='1'"
```

Vi stiller nu altså ikke mere betingelsen, at passwordet skal være lig med den indtastede værdi. Blot at det skal være lig med "" ELLER, at 1 skal være det samme som 1, hvilket det jo til enhver tid vil være. Resultatet er, at vi nu har adgang til den første brugers profil, uden at kende hans/hendes password. Dette er naturligvis meget uheldigt, men løsningen er gudskelov ligeså simpel, som problemet er kritisk. Hele balladen skyldes nemlig den lille single quot ('). Denne skal ved brug i SQL-sætninger erstattes med to af slagsen (''). Dette gøres således.

```
Brugernavn = Replace(Request.Form("brugernavn"), "'", "''")
Password = Replace(Request.Form("password"), "'", "''")
```

Og så er dette problem pludselig ikke længere eksisterende.

Et godt eksempel på omtalte sikkerhedshul fandtes på mødestedet ensomikoebenhavn.dk umiddelbart efter, de havde lanceret siden. Dette ses af følgende screenshot.
http://www.opfinderen.dk/images/articles/ensomikoebenhavn.jpg

Har alt dette givet dig lyst til at forbedre sikkerheden i dit system yderligere, kan du f.eks. stille dig selv følgende spørgsmål.

- Sendes brugerens indtastninger i formularen til serveren i plain text (uden kryptering etc.)?
- Kan du downloade din eventuelle Access-database ved at skrive stien i browseren?
- Er serverens software opdateret, og er den opsat sikkerhedsmæssigt korrekt?

Kommentar af steen d. 15. Jan 2004 | 1

Kommentar af karsten_larsen d. 27. Jan 2004 | 2

En okay artikel - som indfri sin overskrift.

Kommentar af kelo d. 18. Feb 2004 | 3

Kommentar af kingmedia d. 15. Feb 2004 | 4

Glimrende artikel, dog synes jeg at man bør nævne, at gi sine formfelter og db felter andre navne end de gængse "user", "username", "bruger", "brugernavn" osv. :o)

Kommentar af tuctoh d. 15. Jan 2004 | 5

En brugbar artikel, om SQL injektion. Hvis du ikke ved hvad SQL injektion er - skal denne artikel læses!

Kommentar af -sippo- d. 20. Jan 2004 | 6

Kunne godt bruge lidt mere om sikker hed.
Fks. kryptering af text som du selv nævner.
Men ellers meget god.

Kommentar af cade.dk d. 24. Apr 2006 | 7

Ikke 5 point værd.

Kommentar af michaeltajo d. 14. Nov 2005 | 8

Kommentar af asdffdsa d. 16. Jan 2004 | 9

Kommentar af squashguy d. 01. Feb 2004 | 10

Godt at påpege dette! Husk dog at AND har præcedens over OR; hvorfor eksemplet vil logge os ind som den først registrede bruger (som ikke nødvendigvis er Peter)..

Kommentar af sandbox d. 31. Jan 2004 | 11

Bør læses! Også relevant for brugere af andre sprog og andre databaser.

Kommentar af phil-profil d. 13. Mar 2007 | 12

bib

Kommentar af ohhelpme d. 24. Jul 2008 | 13

hva skal man bruge det der til
kunne i det menste lave et eksempel på hvordan man overhovet laver et log ind system