Nem sikkerhed med array()

I denne guide kan du læse om hvordan du nemt med array() kan lave en sikkerhed mod hacking/spam af dit site.

Skrevet den **08. May 2011** af **dab93** I kategorien **Programmering / Andre** | ★★☆☆☆

Array kan bruges til at splitte ting med, og det kan også bruges til en masse andre ting.

Nu siger vi f.eks. at du har et kommentar script, og du har fået en masse spam beskeder med forskellige scripts, og du gerne vil have ændret det så der ikke fremkommer flere irriterende spam scripts.

PHP scripts forekommer tit med apostroffer (') og situations tegn ("). Med array() kan du fjerne muligheden for at disse scripts fungere, og ødelægger din side.

```
$array = array("<", ">", ";", "'");
$array2 = array("&#60;", "&#62;", "&#59;", "&#39;");
```

Her kan du se at $array2 erstatter $array med html charters. Det er en god sikkerhed.
Hele koden:

```
$array = array("<", ">", ";", "'");
$array2 = array("&#60;", "&#62;", "&#59;", "&#39;");

for($i = 0; $i<count($array); $i++) {
  $_POST = str_replace($array[$i], $array2[$i], $_POST);
}
```

Denne kode fungere kun med php variablen $_POST. Det kan også bruges i login, og på den måde sikre mod hacking.

Kommentar af keysersoze d. 07. May 2011 | 1

idéen med at forklare om arrays er god nok, men i forbindelse med sikkerhed mener jeg ikke helt det holder for det kræver at man ved hvad man skal sikre imod. I mine øjne findes der klart lettere metoder end ovenstående - ved input til databasen findes der gode databaseværktøjer, fx prepared statements, og ved visning af potentielt farlige data til klienten findes også færdig funktionalitet på PHP-siden, fx htmlspecialchars.

Kommentar af dab93 d. 07. May 2011 | 2

Sikkerheden er at man i visse tilfælde kan "logge sig ind" på siden, uden at have et ID, og være totalt anonym ved at skrive

```
' OR '1' = '1
```

som eksempel i password feltet. Måske skal der stå noget lidt andet, men det er noget i den stil. Men hvis man bruger sådan et array(), så kan den sikre mod apostroffer ved hacking af siden :).

Kommentar af dab93 d. 07. May 2011 | 3

Rettelse:

```
' OR 1'
```

Kommentar af keysersoze d. 07. May 2011 | 4

Det hedder SQL Injection og kan (= bør) løses af systemer beregnet til det fremfor hjemmelavet funktionalitet der, potentielt set, kan være lige så usikre, og netop prepared statements til MySQL eller parameters til MSSQL er beregnet til dette.

Hvis man replacer risikerer man også utilsigtet at manipulere med brugeres input på en uheldig måde - forestil dig fx at du replacer med html-entiteter inden du gemmer data i databasen og du pludselig skal bruge disse data i andet end en webapplikation.

Nu er jeg ikke den store PHP-haj, men skulle din kode give mening burde $array2 vel enten indeholde html-entiteter fremfor de præcis samme værdier som $array eller også skulle der benyttes htmlentities() i replacen?

Kommentar af dab93 d. 08. May 2011 | 5

#4
Ja du har helt ret med min array, jeg kom til at lave en fejl. Jeg går ind og retter det med det samme.

Kommentar af jaze d. 09. May 2011 | 6

Jeg bliver nødt til at bakke op omkring keysersoze's statement. En almindelig replace er ikke nok, derimod bør man sikre sig med inputvalidering her kan man sikre sig rigtig fornuftigt med f.eks regularexpressions(regex).

Din OR sætning er en af de ældst kendte SQL injections, men desværre gældende, da man afbryder den SQL string der sendes og oftest eksekveres af serveren(server rights) igen her kan man med meget stor fordel benytte forskellige database connectors med "begrænsede" rettigheder til netop den opgave der skal bruges.

Kommentar af wanze d. 11. May 2011 | 7

De arrays du benytter dig af er blot "dårligere" udgaver af PHP-funktionerne `mysql_real_escape_string()` og `htmlentities`.

Kommentar af DSDM d. 20. May 2011 | 8

I .net bruger man jo parametre for at sikre imod injections (: og htmlEncode for at sikre imod at nogen skriver tags/scripts i tekst felter