Spambeskyt formular

Lær en måde at beskytte en formular mod spam.

Skrevet den **03. Feb 2009** af **coderdk** I kategorien **Programmering / PHP** | ⭐⭐⭐☆☆

Der har været en del spørgsmål fra folk der har været udsat for spamangreb i gæstebøger, tagwalls osv. Der findes flere måder at beskytte sig på, og man kan anvende kombinationer af flere løsninger. Her vil jeg demonstrere en simpel CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart).

Metoden kræver GD-lib med png. Du kan ændre det til jpeg eller andet billedformat, hvis du ønsker det.

Jeg håber at scriptet i sig selv, sammen med mine små kommentarer er nok til at gøre scriptet forståeligt.

Scriptet kan du paste til en fil:

```
<?php

    session_start();

    function outputImage()
    {
        // Denne funktion skriver et billede til browseren
        header( 'Content-Type: image/png' );
        $im = imagecreate( 60, 20 );
        // Baggrundsfarven
        $bgcol = imagecolorallocate( $im, 255, 255, 255 );
        // Rammen
        $bordercol = imagecolorallocate( $im, 0, 0, 0 );
        // Tekstfarce
        $textcol = imagecolorallocate( $im, 100, 100, 220 );
        // Fyld med baggrundsfarven
        imagefill( $im, 1, 1, $bgcol );
        for ( $i = 0; $i < 4; $i++ )
        {
            // Tilfældig farve til linjerne
            $tmpCol = imagecolorallocate(
                $im, mt_rand( 100, 230), mt_rand( 100, 230), mt_rand( 100,
230) );
            // Tegn linje
            imageline( $im, 0, mt_rand( 0, 19 ), 59, mt_rand( 0, 19 ), $tmpCol
);
        }
        // Skriv CAPTCHA-teksten
        imagestring( $im, 5, 9, 2, $_SESSION['captcha-code'], $textcol );
        // Wave effect
        for ( $i = 0; $i < 60; $i += 2 )
            imagecopy( $im, $im, $i - 2, sin( $i / 10 ) * 3, $i, 0, 2, 20 );
```

```
        // Tegn rammen
        imagerectangle( $im, 0, 0, 59, 19, $bordercol );
        // Smid billedet til browseren
        imagepng( $im );
        imagedestroy( $im );
        // Stop scriptet her!
        exit;
    }

    function newCode()
    {
        // Denne funktion laver en tekst der (som regel) kan udtales
        $vowels = array_slice( preg_split( '//', 'AEUY' ), 1, -1 );
        $nvowels = count( $vowels ) - 1;
        $consonants = array_slice( preg_split( '//', 'BCDFGHJKLMNPQRSTVWXZ' ),
1, -1 );
        $nconsonants = count( $consonants ) - 1;
        $code = "";
        $rnd = mt_rand( 0, 1 ) == 1 ? true : false;
        // Loopet herunder bygger teksten
        while ( strlen( $code ) < 5 )
        {
            $code .= ( $rnd ? $vowels[ mt_rand( 0, $nvowels ) ]
                : $consonants[ mt_rand( 0, $nconsonants ) ] );
            $rnd = !$rnd;
        }
        // Smid teksten i en sessionsvariabel
        $_SESSION['captcha-code'] = $code;
    }

    if ( isset( $_GET['img'] ) || isset( $_GET['newimg'] ))
    {
        if ( isset( $_GET['newimg'] ) )
        {
            // Brugeren kunne ikke læse koden, så lav en ny
            newCode();
        }
        // Vis billede
        outputImage();
        // Scriptet stopper i outputImage() - Denne kode bliver altså kun
        // kørt når der gives ?img eller ?newimg i URL'en
    }

    // Dan ny CAPTCHA-tekst
    newCode();

?>
<script type="text/javascript">
    function getNewImg()
    {
        var d = new Date();
        document.getElementById('theImg').src =
            '<?= $_SERVER['PHP_SELF'] ?>?newimg&x' + d.getTime();
    }
</script>
```

```
<form method="post" action="formhandler.php">
    <img id="theImg" align="top" src="<?= $_SERVER['PHP_SELF'] ?>?img">
    <input type="button" value="Jeg kan ikke læse det!"
onclick="getNewImg()"><br>
    Skriv bogstaverne i billedet:
    <input type="text" style="width: 60px" name="kode">
    <input type="submit" value="Indsend">
</form>
```

Formularen er sat til at POST'e til formhandler.php, som i mit eksempel kun indeholder:

```
<?php

    session_start();

    if ( !empty( $_POST['kode'] ) && strtoupper( $_POST['kode'] ) ==
$_SESSION['captcha-code'] )
    {
        // Koden brugeren tastede var korrekt, og du kan nu gemme hvad han har
postet
    }
    else
    {
        $_SESSION['captcha-code'] = md5( microtime() );
        echo "<p>Desværre, koden du skrev, var forkert. Prøv igen.</p>";
    }

?>
```

Det er sådan set det hele.

Distributed Sender Blackhole List

Der er en enkelt anden metode, som jeg kort vil komme ind på: Sitet www.dsbl.org - Distributed Sender Blackhole List. Sitet er en database over IP'er der er registreret som åbne relay mailservere. Disse er typisk zombier og bliver brugt af mange spammere. Der er en ganske simpel metode til at teste om en IP er registreret hos dem:

```
<?php

    list($a, $b, $c, $d) = explode( '.', $_SERVER['REMOTE_ADDR'] );
    if ( checkdnsrr( "$d.$c.$b.$a.list.dsbl.org" ) )
    {
        header( "Location: http://dsbl.org/listing?" . $_SERVER['REMOTE_ADDR']
);
        exit;
    }
```

```
?>
```

Koden checker om der findes en DNS-record på dsbl.org's DNS, der indikerer at klientens IP er listet hos dem. Er den det, er det med rimelig sikkerhed et åbent relay (potentiel mail spammer).

Denne metode virker på nogle servere, men på min egen server virker den ikke helt efter hensigten. Hvis det ikke virker for dig, så prøv med:

```
<?php

    list($a, $b, $c, $d) = explode( '.', $_SERVER['REMOTE_ADDR'] );
    if ( gethostbyname( "$d.$c.$b.$a.list.dsbl.org" ) == '127.0.0.2' )
    {
        header( "Location: http://dsbl.org/listing?" . $_SERVER['REMOTE_ADDR']
);
        exit;
    }

?>
```

Det virker på min egen server.

Begge scripts sender brugeren videre til www.dsbl.org til en side der fortæller at de er registreret som værende et åbent relay, og hvad de kan gøre for at komme af denne liste...

dsbl.org opretter alle registrerede IP'er (a.b.c.d) som d.c.b.a.list.dsbl.org i deres DNS-server, ved at teste om adressen er i deres DNS ved vi at de er listet hos dem.

Det var lige hvad jeg havde her! Feedback er velkomment.

Update: Der er nu en fast bølgeeffekt, for at gøre det lidt mere besværligt for eventuelle bots...

Kommentar af philip d. 19. Sep 2006 | 1

Rigtig god artikel! Thumbs up!

Kommentar af htx98i17 d. 24. Jan 2009 | 2

Copy/pastet og det fungerer.

Kommentar af cf560 d. 25. Nov 2006 | 3

Kommentar af gider_ikke_mere d. 28. May 2007 | 4

Fin artikel, men for de uøvede burde eksemplet måske indeholde HTML-koden for at vise hvorledes de forskellige funktioner skal placeres på siden.
For de der ønsker en større og/eller anden font , kan man rette følgende linie:

imagestring($im, 5, 9, 2, $_SESSION['captcha-code'], $textcol);

til:

$font = imageloadfont("arial_unicode_ms22.gdf");
imagestring($im, $font, 9, 2, $_SESSION['captcha-code'], $textcol);

arial_unicode_ms22.gdf er en PHP filfont jeg kreerede med et lille program: "Windows font to PHP font", fundet her: http://dk2.php.net/manual/da/function.imageloadfont.php#72223 eller downloadet her: http://www.wedwick.com/wftopf.exe
akyhne

Kommentar af jakobdo d. 31. Oct 2006 | 5

God artikel! Og som andre er inde på: Gratis er godt.

Kommentar af miffe d. 10. Jan 2007 | 6

Rigtig lækker artikel. Jeg takker herfra.

Kommentar af serverservice d. 01. Oct 2006 | 7

Fedeste artikel - og endda gratis - jeg må lige se nærmere på hvad jeg kan få brug for til en af mine CMSér og da er den god til inspiration.

Kommentar af miqe d. 18. Sep 2006 | 8

Overvejede faktisk at lave et php-script af ovenstående type, til at sortere skidt fra kanel. Dette kommer til at spare mig fra at opfinde den dybe tallerken igen igen.
Fedt at få en quick ´n dirty artikel om at slippe for SPAM´ere.

Kommentar af mik2000 d. 16. Sep 2007 | 9

Rigtig flot artikel. Godt beskrevet. Men det script der tjekker om ip er registreret på den server. Hvordan tester man om det virker?
Hvordan får man skriften større end 5?

Kommentar af scarface335 d. 18. Sep 2006 | 10

Kommentar af showsource d. 19. Nov 2006 | 11

Nice !!!
Og www.dsbl.org kendte jeg ikke :O)

Kommentar af psycho42 d. 08. Oct 2006 | 12

Rigtig nice - og gratis :o) - Life is sharing ;)

Kommentar af super-mann d. 22. Jan 2007 | 13

Rigtig god artikel, vejledning og script - som bare virker! Ikke haft spam på min side i nu 48 timer, succes! Modtog før ca. 4-5 indlæg i timen. Noget jeg kunne ønske mig, ville være mulighed for større jpeg fil, da teksten er ret lille.