OWASP-DK CTF #1

PRICEWATERHOUSECOOPERS

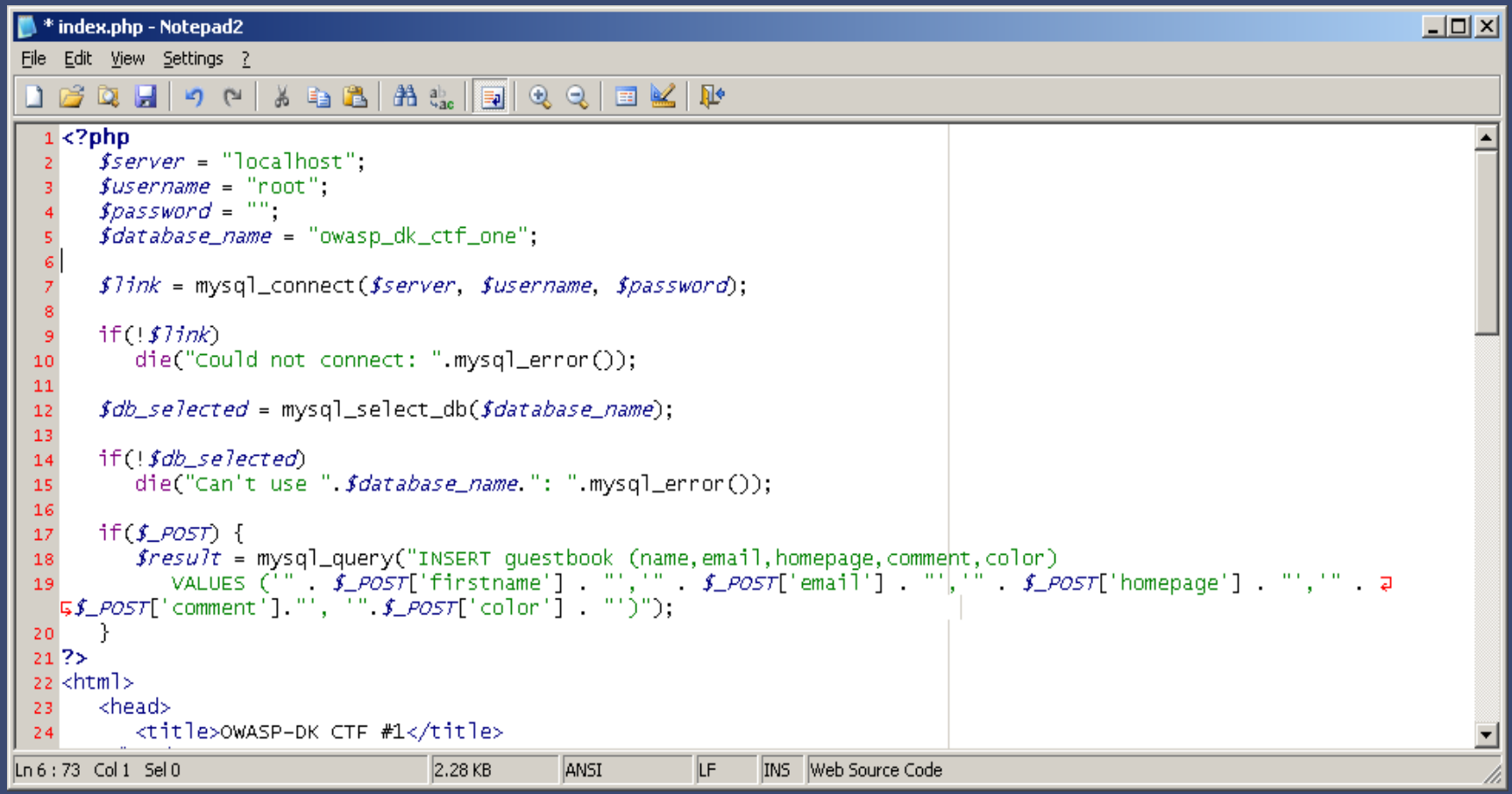
Om OWASP-DK CTF #1

- Gæstebog
- Navn
- Email
- Website
- Kommentar
- Valg af baggrundsfarve til kommentar-feltet
- White box / source code review
- Antal linjer kode: 73 (SLOC/KLOC)

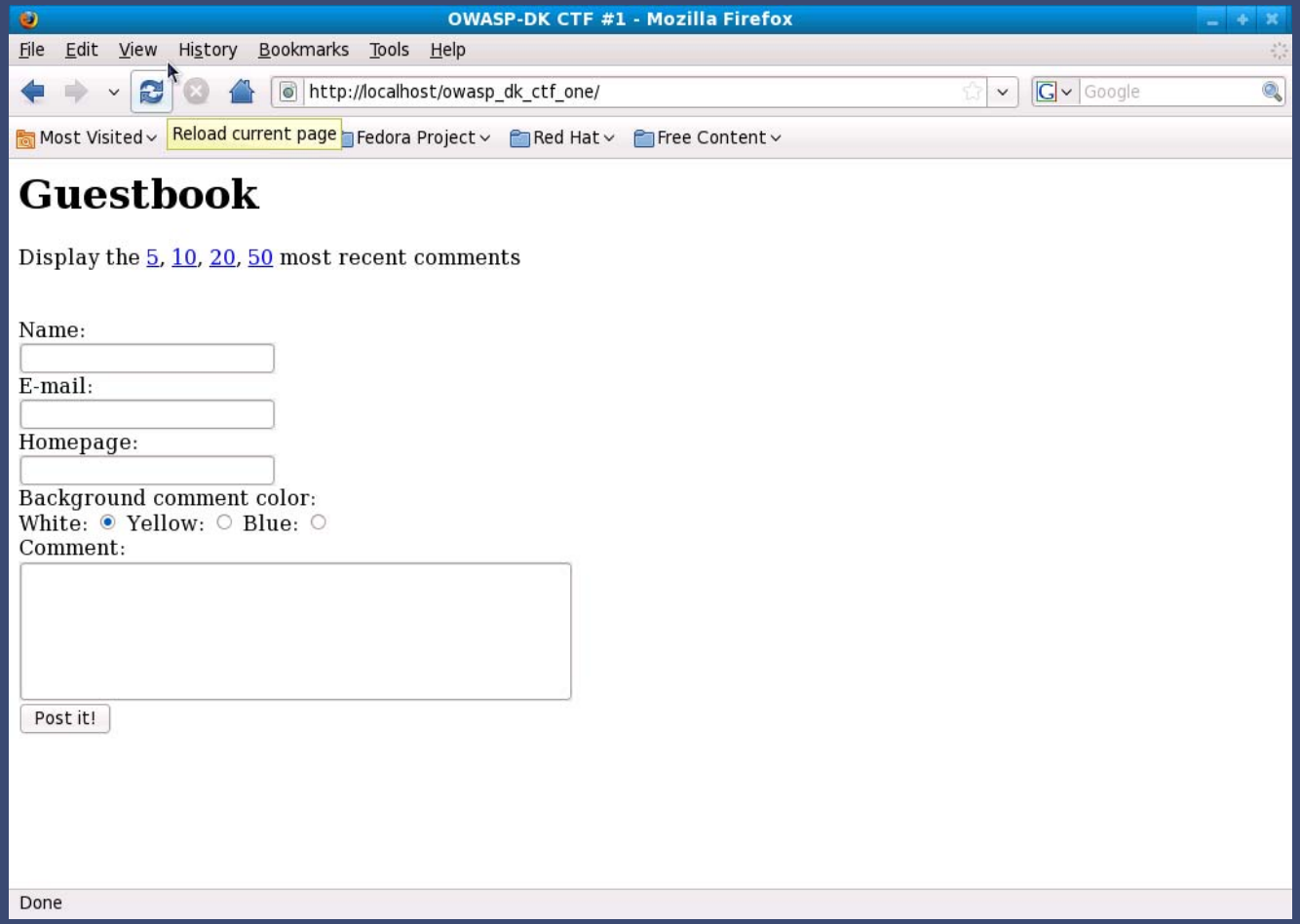
Krav

- PHP
- MySQL
- `magic_quotes_gpc` skal være slået fra I `php.ini`

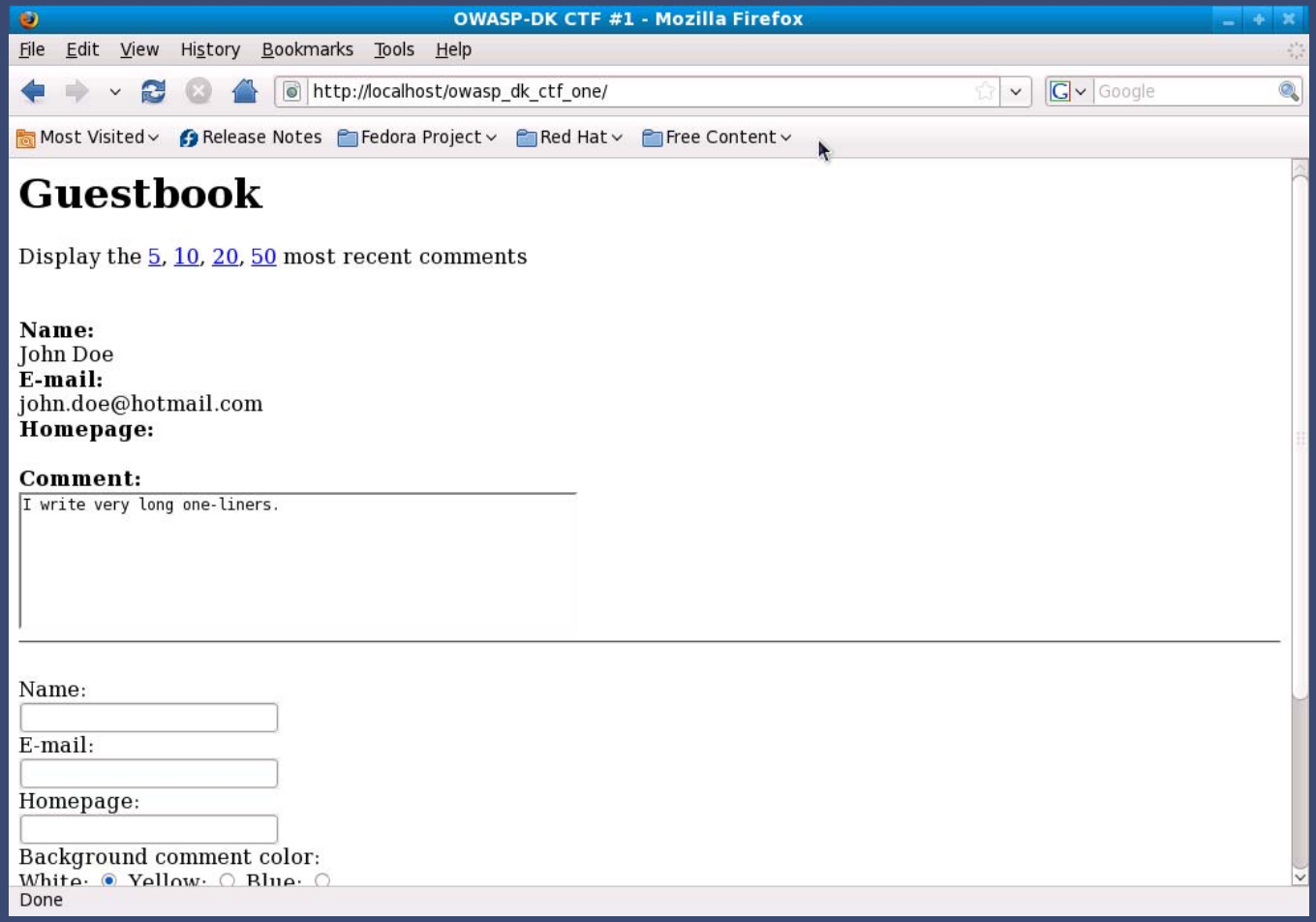
Koden


* index.php - Notepad2
File Edit View Settings ?
<?php
$server = "localhost";
$username = "root";
$password = "";
$database_name = "owasp_dk_ctf_one";
$link = mysql_connect($server, $username, $password);
if(!$link)
die("Could not connect: ".mysql_error());
$db_selected = mysql_select_db($database_name);
if(!$db_selected)
die("Can't use ".$database_name.": ".mysql_error());
if($_POST) {
$result = mysql_query("INSERT guestbook (name,email,homepage,comment,color)
VALUES ('" . $_POST['firstname'] . "','" . $_POST['email'] . "','" . $_POST['homepage'] . "','" .
$_POST['comment']."', '".$_POST['color'] . "')");
}
?>
<html>
<head>
<title>OWASP-DK CTF #1</title>
Ln 6 : 73 Col 1 Sel 0
2.28 KB
ANSI
LF
INS
Web Source Code

Gæstebogen (screenshot 1)



Gæstebogen (screenshot 2)



Opgaveløsning

Opgaveløsninger bør indeholde:

- Hvilke sårbarheder eksisterer i gæstebogen?
  - Observation
  - Risiko
  - Risikoniveau
- Hvordan udnyttes sårbarhederne?
  - Beskrivelse
  - evt. scripts / moduler til Metasploit, W3AF, osv.
- Anbefalinger til sikkerhedsmæssige forbedring af gæstebogen
- En version af gæstebogen hvor de fundne sårbarheder er udbedret

Hvor kan OWASP-DK CTF #1 hentes fra?

- http://joes.anarcho.dk/ctf/owasp/owasp_dk_ctf1.zip
- http://rasmuspetersen.net/owasp_dk_ctf1.zip

MD5sum: ba0c0069df1648895ce269e960415122

Deadline

- Start: nu!
- Deadline: 1/8 – 2009
- Opgaveløsninger skal sendes til nedenstående email-adresse:
- pragmatk@attackresearch.com
- Evt PGP:
  Fingerprint (nøgle 0x323C7837):
  6426 C563 2592 0BB8 5193 797E 1A09 9E97 323C 7837

Præmie

- Et par øl fra Mikkeller-bryggeriet

Dommere

- Martin Clausen (Deloitte)
- Joe / “Pragmatk”
- Rasmus Petersen (PwC)