

Forum:[Hack Forums](#)

Thread: [This Backdoor Won a DEFCON 23 Contest - Can You Figure it Out?](#)

sarciszewski - January 7, 2016, 7:02 pm

The challenge:

Spoiler ([Click to View](#))

To clarify the usability, assume that your document root is set to public/, such that <http://somedomain.com/foo.php> resolves to public/foo.php, not foo.php.

```
autoload.php
PHP Code
<?php
/**
 * Too lazy to do a PSR-4 autoloader using spl_autoload(), we only have one
 * class anyway.
 *
 *
 *                                     Scott Arciszewski
 */
require_once "TimingSafeAuth.php";

/**
 * Generate a random string with our specific charset, which conforms to the
 * RFC 4648 standard for BASE32 encoding.
 *
 * @return string
 */
function noise()
{
    return substr(
        str_shuffle(str_repeat('abcdefghijklmnopqrstuvwxyz234567', 16)),
        0,
        32
    );
}

TimingSafeAuth.php:
PHP Code
<?php

/**
 * A password_* wrapper that is proactively secure against user enumeration from
 * the timing difference between a valid user (which runs through the
 * password_verify() function) and an invalid user (which does not).
 */
class TimingSafeAuth
{
    private $db;
    public function __construct(\PDO $db)
```

```

{
    $this->db = $db;
    $this->dummy_pw = password_hash(noise(), PASSWORD_DEFAULT);
}

/**
 * Authenticate a user without leaking valid usernames through timing
 * side-channels
 *
 * @param string $username
 * @param string $password
 * @return int|false
 */
public function authenticate($username, $password)
{
    $stmt = $this->db->prepare("SELECT * FROM users WHERE username = :username");
    if ($stmt->execute(['username' => $username])) {
        $row = $stmt->fetch(\PDO::FETCH_ASSOC);
        // Valid username
        if (password_verify($password, $row['password'])) {
            return $row['userid'];
        }
        return false;
    } else {
        // Returns false
        return password_verify($password, $this->dummy_pw);
    }
}
}

```

public/index.php:

PHP Code

```
<?php
```

```

require_once dirname(__DIR__).'/autoload.php';
$db = new \PDO('sqlite:'. dirname(__DIR__) . '/database.sql');
session_start();

```

```

if (!isset($_SESSION['userid'])) {
    if (!empty($_POST['csrf']) && !empty($_COOKIE['csrf'])) {
        if (hash_equals($_POST['csrf'], $_COOKIE['csrf'])) {
            $auth = new TimingSafeAuth($db);
            $userid = (int) $auth->authenticate($_POST['username'], $_POST['password']);
            if ($userid) {
                // Success!
                $_SESSION['userid'] = $userid;
                header("Location: /");
                exit;
            }
        }
    }
}
require_once dirname(__DIR__).'/secret/login_form.php';
} else {
    require_once dirname(__DIR__).'/secret/login_successful.php';
}

```

```
}
```

secret/login_form.php

PHP Code

```
<?php
if (!isset($_COOKIE['csrf'])) {
    $csrf = noise();
    setcookie('csrf', $csrf);
} else {
    $csrf = $_COOKIE['csrf'];
}
?>
<!DOCTYPE html>
<html>
<head>
    <title>Log In</title>
    <link rel="stylesheet" href="/style.css"?<?=rand(); ?>" type="text/css" /><?php
/* cache-busting random query string */ ?>
</head>
<body>
<form method="post" action="/">
    <input type="hidden" name="csrf" value="<?=htmlentities($csrf, ENT_QUOTES | ENT_HTML5,
'UTF-8'); ?>" />
    <table>
        <tr>
            <td>
                <fieldset>
                    <legend>Username</legend>
                    <input type="text" name="username" required="required" />
                </fieldset>
            </td>
            <td>
                <fieldset>
                    <legend>Password</legend>
                    <input type="password" name="password" required="required" />
                </fieldset>
            </td>
        </tr>
        <tr>
            <td colspan="2">
                <button type="submit">
                    Log In
                </button>
            </td>
        </tr>
    </table>
</form>
</body>
</html>
```

secret/login_successful.php

PHP Code

```
<?php
```

```
<!DOCTYPE html>
<html>
<head>
  <title>Welcome</title>
  <link rel="stylesheet" href="/style.css?<?=rand(); ?>" type="text/css" /><?php
/* cache-busting random query string */ ?>
</head>
<body><?php
if ($_SESSION['userid'] == 1) {
  echo "Welcome great leader!\n";
  echo "<hr />";
  echo "Administrative features: ...";
  /**
   * @todo make the admin account actually useful ;)
   */
} else {
  echo "Welcome, peon.\n";
}
?></body>
</html>
```

The full write-up is available online. Don't feel bad if you can't figure it out at first glance.

Spoiler: [On The Design and Implementation of a Stealth Backdoor for Web Applications](#)

So, no takers? Is this too difficult for everyone?