XSS in setup.php - PhpMyAdmin 2.11.7

Discovered by: Aung Khant
Date: July 17, 2008
Product: PhpMyAdmin 2.11.7 (http://phpmyadmin.net)
Vulnerability Type: Cross-Site Scripting (XSS)
Risk: **N/A**
Threats: N/A

Note:

An XSS baby has been born in

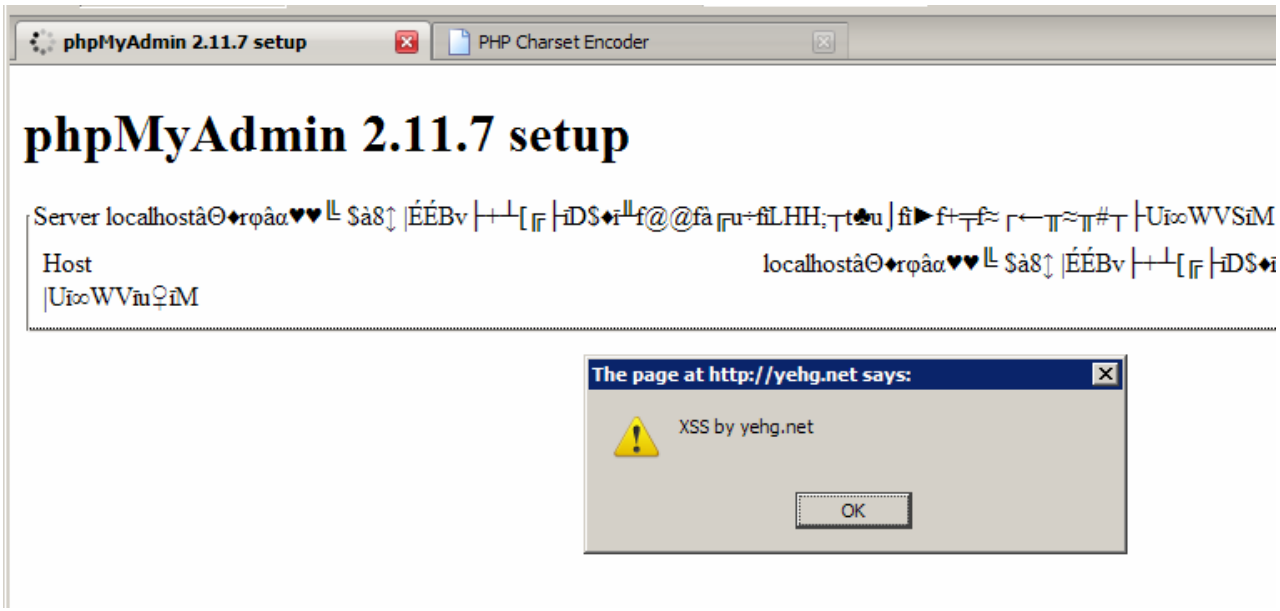
/phpMyAdmin-2.11.7-english/scripts/setup.php

due to the lack of HTML Escape:

At function -> show_overview ($title, $list, $buttons = '')
At Line -> 685,
At Code -> echo $val[1];

```
675 */
676 function show_overview($title, $list, $buttons = '') {
677     echo '<fieldset class="overview">' . "\n";
678     echo '<legend>' . $title . '</legend>' . "\n";
679     foreach ($list as $val) {
680         echo '<div class="row">';
681         echo '<div class="desc">';
682         echo $val[0];
683         echo '</div>';
684         echo '<div class="data">';
685         echo $val[1];
686         echo '</div>';
687         echo '</div>' . "\n";
688     }
689     if (!empty($buttons)) {
```

Proof-of-Concept:



This is a kind of Stored XSS. In order to execute XSS on the victim admin, the following criteria must be met:

1) The scripts and the config folder have not been deleted yet.
2) A victim admin sometimes uses scripts/setup.php for generating configuration file. As an example case, a server admin generates phpMyAdmin config file from his default web site (which is accessible only via IP address) whenever new customer purchases a web hosting package.
3) An attacker overwrites config/config.php with malicious obfuscated XSS payload.
4) After the victim clicks “Load” and “List” to view overall configurations, he gets xssed.

There seems to have little chance of XSS execution. Nevertheless, with an intelligent masked Social Engineering, a smart attacker may induce a victim admin to execute XSS and leverages this to do scanning the victim’s internal network, network drives, stealing browser histories and exploiting other web hosting administration packages weaknesses.

In real-world hacking 0wnage news, attackers managed to gain access in spite of very tight constraint of access and very low possibility of access.