qdPM9.1 Installer Cross-Site-Scripting

一、 背景介绍

qdPM是一个免费的基于Web的项目管理工具，适用于从事多个项目的小团队。可自由配置，从而轻松管理项目，任务和人员。

1.1 漏洞描述

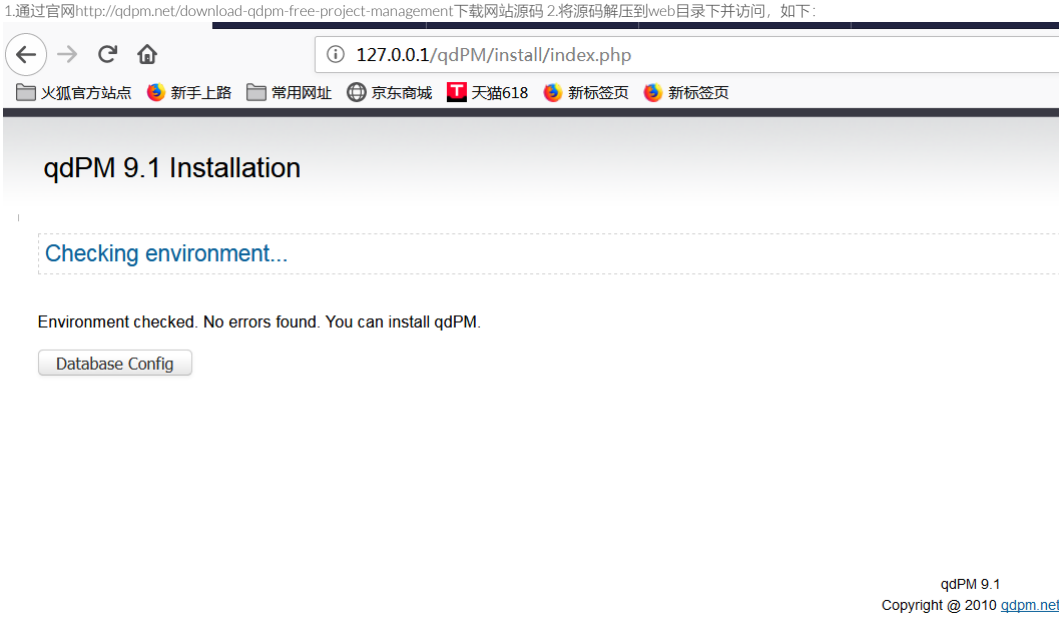
qdPM安装页面由于参数过滤不严格，导致反射型xss。

1.2 受影响的系统版本

qdPM 9.1

二、环境搭建

1.通过官网http://qdpm.net/download-qdpm-free-project-management下载网站源码 2.将源码解压到web目录下并访问，如下：



三、漏洞分析

网站安装过程中的数据库配置文件为qdPM\install\modules\database_config.php，如下图所示，可以看到当db_error为真时，会将db_error的值输出到页面，在此过程中，没有进行任何过滤，这导致了发射型xss：

```
19   * needs please refer to http://www.qdPM.net for more information.
20   *
21   * @copyright  Copyright (c) 2009  Sergey Kharchishin and Kym Romanets (http://www.qdpm.net)
22   * @license    http://opensource.org/licenses/osl-3.0.php  Open Software License (OSL 3.0)
23   */
24  ?>
25  <div class="infoBlock"><h1>Database config</h1></div>
26
27  <?php if($_GET['db_error']) echo '<div class="error_text">'. $_GET['db_error'] .'</div>';?>
28
29 <form name="db_config" action="index.php?step=qdpm_config" method="post">
30 <table class="formTable">
31   <tr>
32     <td>Database host:</td>
33     <td><input type="text" name="db_host" id="db_host" value="localhost"></td>
34     <td>The address of the database server in the form of a hostname or IP address.</td>
35   </tr>
36   <tr>
37     <td>Database port:</td>
38     <td><input type="text" name="db_port" id="db_port" value=""></td>
39     <td>MySQL Connection Port. <i>(Leave this blank unless you know the server operates on a non-standard p
40   </tr>
41   <tr>
42     <td>Database name:</td>
43     <td><input type="text" name="db_name" id="db_name" value="qdpm"></td>
44     <td>The name of the database to hold the data in.</td>
45   </tr>
46   <tr>
```

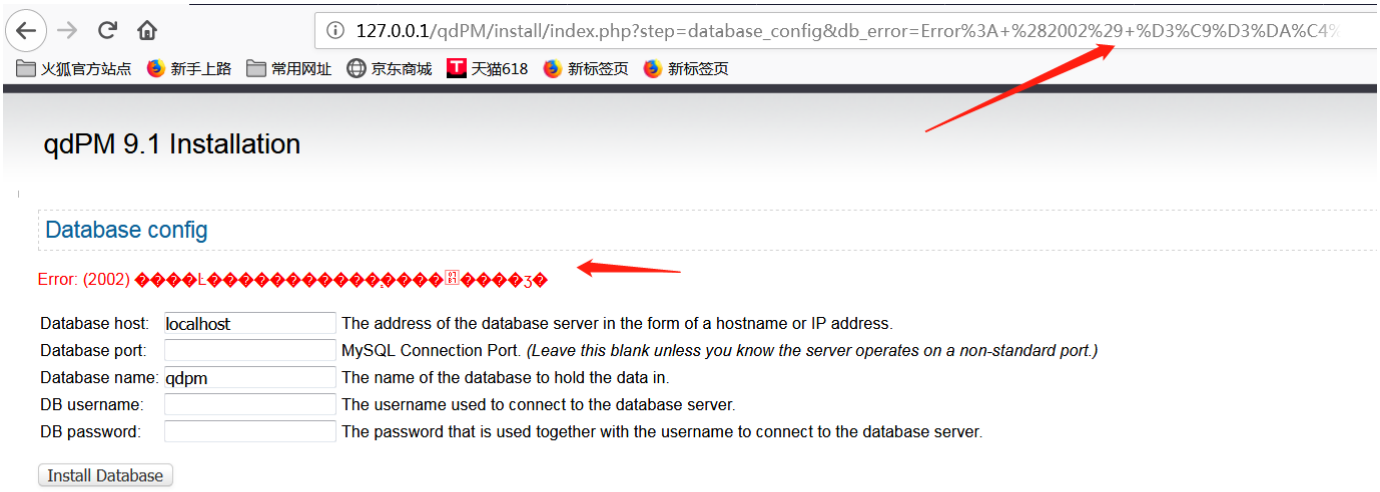
四、漏洞利用

1.访问网站：

2.点击database config按钮并输入错误的数据

库信息：

3.提交之后，我们可以看到db_error信息输出在页面上：



4.构造

payload url：http://127.0.0.1/qdPM/install/index.php?step=database_config&db_error= 并对其访问

5.可以看到，xss成功执行：