BigTiger2020 Rename Fantastic-Blog-CMS-2 to Fantastic-Blog-CMS-2.md History

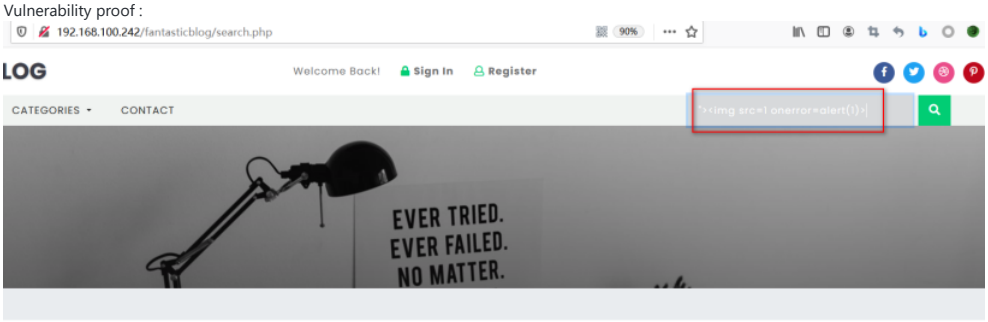
1 contributor

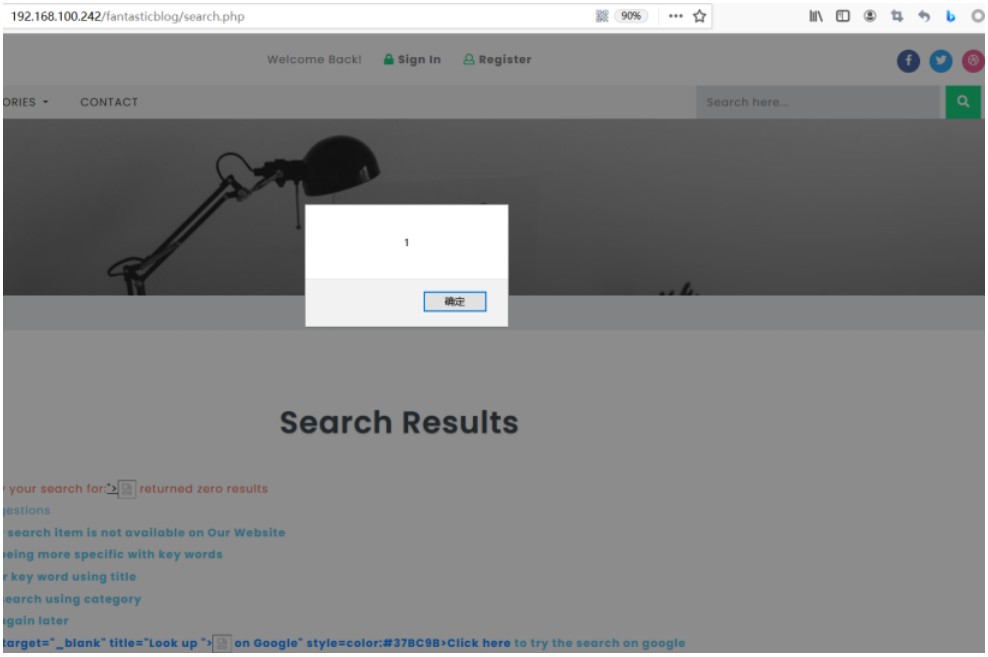
9 lines (9 sloc) | 627 Bytes

- Exploit Title: Fantastic-Blog-CMS 1.0- Reflective cross-site scripting
- Vendor Homepage: https://www.sourcecodester.com/php/12258/fantastic-blog-cms-php.html
- Software Link:https: https://www.sourcecodester.com/download-code?nid=12258&title=Fantastic+Blog+%28CMS%29+in+PHP+with+Source+Code
- Version: 1.0
- Vulnerable file: search.php

```php
<?php
$search_keyword = '';
if(!empty($_POST['search']['keyword'])) {
    $search_keyword = $_POST['search']['keyword'];
}
$sql = 'SELECT * FROM blogs WHERE title LIKE :keyword OR content LIKE :keyword  OR tags LIKE :keyword OR author LIKE :keyword ORDER BY id DESC ';

/* Pagination Code starts */
$per_page_html = '';
$page = 1;
$start=0;
if(!empty($_POST["page"])) {
    $page = $_POST["page"];
    $start=($page-1) * ROW_PER_PAGE;
}
$limit=" limit " . $start . "," . ROW_PER_PAGE;
$pagination_statement = $pdo_conn->prepare($sql);
$pagination_statement->bindValue(':keyword', '%' . $search_keyword . '%', PDO::PARAM_STR);
$pagination_statement->execute();

$row_count = $pagination_statement->rowCount();
if(!empty($row_count)){
    $per_page_html .= "<div style='text-align:center;margin:20px 0px;'>";
    $page_count=ceil($row_count/ROW_PER_PAGE);
    if($page_count>1) {
        for($i=1;$i<=$page_count;$i++){
            if($i==$page){
                $per_page_html .= '<input type="submit" name="page" value="' . $i . '" class="btn-page current btn-warning" />';
            } else {
                $per_page_html .= '<input type="submit" name="page" value="' . $i . '" class="btn-page btn-danger" />';
            }
        }
    }
    $per_page_html .= "</div>";
}

$query = $sql.$limit;
$pdo_statement = $pdo_conn->prepare($query);
$pdo_statement->bindValue(':keyword', '%' . $search_keyword . '%', PDO::PARAM_STR);
$pdo_statement->execute();
$result = $pdo_statement->fetchAll();
?>
```

- Vulnerability proof :




192.168.100.242/fantasticblog/search.php
90%
Welcome Back!
Sign in
Register
CONTACT
Search here...
1
确定
Search Results
returned zero results
search item is not available on Our Website
key word using title
again later
on Google" style=color:#37BC9B>Click here to try the search on google