

МИНОБРНАУКИ РОССИИ
федеральное государственное автономное образовательное учреждение высшего
образования «Самарский национальный исследовательский университет
имени академика С.П. Королева»
(Самарский университет)

Институт информатики, математики и электроники
Факультет механико-математический
Кафедра безопасности информационных систем
Дисциплина Модели безопасности компьютерных систем

Лабораторная работа №3

Тема: Ознакомление и использование NoSQLMap

Выполнили:

студенты 4 курса, группа 6442-100501D

ФИО:

Стрыгина В.Э.

Молостов О.А.

Круталева И.В.

Проверил: Бурлаков М.Е.

Работа проверена

« » _____ 202__ г.

Оценка _____

Преподаватель _____

СОДЕРЖАНИЕ

| | |
|--|----|
| ВВЕДЕНИЕ..... | 3 |
| 1 Установка программ..... | 4 |
| 1.1 Установка MongoDB..... | 4 |
| 1.2 Настройка NoSQLMap..... | 5 |
| 2 Настройка базы данных..... | 9 |
| ЗАКЛЮЧЕНИЕ | 13 |
| СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ | 14 |

ВВЕДЕНИЕ

Если пользователь использует базу данных NoSQL, такую как MongoDB, и не уверен, что она достаточно хороша (не находит все уязвимости, не видит неправильную конфигурацию), такой инструмент как NoSQLMap поможет ему исправить эту ситуацию.

NoSQLMap — это утилита с открытым исходным кодом, основанная на Python. Она способна проводить аудит для поиска неправильной конфигурации и автоматизации инъекционных атак [1].

Целью данной работы является ознакомление с NoSQLMap.

Для достижения поставленной цели нами были поставлены следующие задачи:

1. установить необходимые программы
2. настроить базу данных.

1 Установка программ

1.1 Установка MongoDB

MongoDB — документоориентированная система управления базами данных, не требующая описания схемы таблиц. Считается одним из классических примеров NoSQL-систем [2].

MongoDB подходит для следующих применений [2]:

- хранение и регистрация событий;
- системы управления документами и контентом;
- электронная коммерция;
- игры;
- данные мониторинга, датчиков;
- мобильные приложения;
- хранилище операционных данных веб-страниц (например, хранение комментариев, рейтингов, профилей пользователей, сеансы пользователей).

Для настройки MongoDB в Kali Linux необходимо использовать команду:

```
wget -qO - https://www.mongodb.org/static/pgp/server-4.2.asc | sudo apt-key  
add – [3]
```

Следующим шагом создаем `/etc/apt/sources.list.d/mongodb-org-4.2.list` файл для MongoDB [3].

Далее выполняем следующую команду, чтобы перезагрузить локальную базу данных пакетов: `sudo apt-get update`. Затем устанавливаем пакеты MongoDB: `sudo apt-get install -y mongodb-org` [4].

Для удобного взаимодействия PHP и MongoDB необходимо установить библиотеку с помощью команды: `composer require mongodb/mongodb`. Данная команда должна вывести:

```
/composer.json has been created  
Loading composer repositories with package information
```

Updating dependencies (including require-dev)

- Installing mongodb/mongodb (1.0.0)

Downloading: 100%

Writing lock file

Generating autoload files

1.2 Настройка NoSQLMap

NoSQLMap — это инструмент на Python с открытым исходным кодом предназначенный для аудита и автоматических инъекционных атак и эксплуатаций слабостей (конфигураций с дефолтными учётными данными) в базах данных NoSQL, а также в веб-приложениях, использующих NoSQL, для вскрытия информации из базы данных [5].

Возможности:

- Атаки автоматического перечисления и клонирования баз данных MongoDB и CouchDB.
- Извлечение имён баз данных, пользователей и хешей паролей из MongoDB через веб-приложения.
- Сканирование подсетей или списка IP в поисках баз данных MongoDB и CouchDB с доступом по умолчанию и перечисление версий.
- Атака по словарю и брут-форсом по взлому паролей выявленных хешей MongoDB и CouchDB.
- Инъекционные атаки на параметры PHP приложений для возврата всех записей базы данных.
- Функция экранирования величин Javascript и инъекции произвольного кода для возврата всех записей базы данных.

- Основанные на тайминге атаки, сходные со слепыми SQL инъекциями, для валидации уязвимостей инъекций Javascript с приложениями без обратной связи.

NoSQLMap можно установить, клонировав их репозиторий из GitHub и запустив скрипт установки [6]:

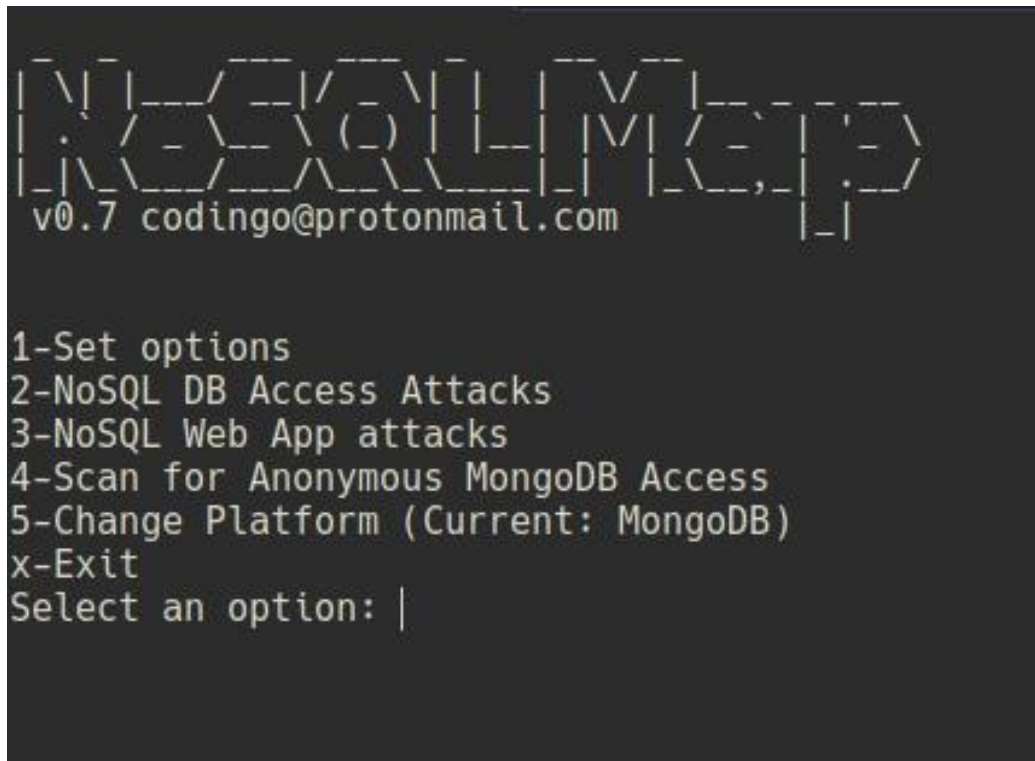
```
git clone https://github.com/codingo/NoSQLMap.git
```

```
cd NoSQLMap
```

```
python setup.py install
```

Для запуска NoSQLMap необходимо запустить команду `./nosqlmap.py`

На рисунке 1 представлено главное меню:



```

NoSQLMap
v0.7 codingo@protonmail.com

1-Set options
2-NoSQL DB Access Attacks
3-NoSQL Web App attacks
4-Scan for Anonymous MongoDB Access
5-Change Platform (Current: MongoDB)
x-Exit
Select an option: |
```

Рисунок 1. Главное меню

Основные опции NoSQLMap изображены на рисунке 2.

```
Options
1-Set target host/IP (Current: Not Set)
2-Set web app port (Current: 80)
3-Set App Path (Current: Not Set)
4-Toggle HTTPS (Current: OFF)
5-Set MongoDB Port (Current : 27017)
6-Set HTTP Request Method (GET/POST) (Current: GET)
7-Set my local MongoDB/Shell IP (Current: Not Set)
8-Set shell listener port (Current: Not Set)
9-Toggle Verbose Mode: (Current: OFF)
0-Load options file
a-Load options from saved Burp request
b-Save options file
h-Set headers
x-Back to main menu
Select an option: |
```

Рисунок 2. Основные опции

Также возможен выбор СУБД (рис. 3).

```
1-MongoDB
2-CouchDB
Select a platform: |
```

Рисунок 3. Выбор СУБД

Подробную информацию можно просмотреть с помощью команды `-help` (рис. 4).

```

(root@kali)-[~/NoSQLMap]
└─# ./nosqlmap.py --help
usage: nosqlmap.py [-h] [--attack {1,2,3}] [--platform {MongoDB,CouchDB}]
                  [--victim VICTIM] [--dbPort DBPORT] [--myIP MYIP]
                  [--myPort MYPORT] [--webPort WEBPORT] [--uri URI]
                  [--httpMethod {GET,POST}] [--https {ON,OFF}]
                  [--verb {ON,OFF}] [--postData POSTDATA]
                  [--requestHeaders REQUESTHEADERS]
                  [--injectedParameter INJECTEDPARAMETER]
                  [--injectSize INJECTSIZE] [--injectFormat INJECTFORMAT]
                  [--params PARAMS] [--doTimeAttack DOTIMEATTACK]
                  [--savePath SAVEPATH]

optional arguments:
  -h, --help                show this help message and exit
  --attack {1,2,3}          1 = NoSQL DB Access Attacks, 2 = NoSQL Web App
                           attacks, 3 - Scan for Anonymous platform Access
  --platform {MongoDB,CouchDB}
                           Platform to attack
  --victim VICTIM           Set target host/IP (ex: localhost or 127.0.0.1)
  --dbPort DBPORT          Set shell listener port
  --myIP MYIP              Set my local platform/Shell IP
  --myPort MYPORT          Set my local platform/Shell port
  --webPort WEBPORT        Set web app port ([1 - 65535])
  --uri URI                Set App Path. For example '/a-path/'. Final URI will
                           be [https option]://[victim option]:[webPort
                           option]/[uri option]
  --httpMethod {GET,POST}  Set HTTP Request Method
  --https {ON,OFF}         Toggle HTTPS
  --verb {ON,OFF}         Toggle Verbose Mode
  --postData POSTDATA      Enter POST data in a comma separated list (i.e. param
                           name 1,value1,param name 2,value2)
  --requestHeaders REQUESTHEADERS
                           Request headers in a comma separated list (i.e. param
                           name 1,value1,param name 2,value2)

nsmweb:
  --injectedParameter INJECTEDPARAMETER
                           Parameter to be injected
  --injectSize INJECTSIZE
                           Size of payload
  --injectFormat INJECTFORMAT
                           1-Alphanumeric, 2-Letters only, 3-Numbers only,
                           4-Email address
  --params PARAMS          Enter parameters to inject in a comma separated list
  --doTimeAttack DOTIMEATTACK
                           Start timing based tests (y/n)
  --savePath SAVEPATH      output file name

```

Рисунок 4. Результат команды help

2 Настройка базы данных

Для запуска MongoDB воспользовались командой `mongod --dbpath /data/db --bind_ip 127.0.0.1 --auth` (рис. 5).

```
(root@kali)~[~/etc/mysql]
└─# mongod --dbpath /data/db --bind_ip 127.0.0.1 --auth
2021-07-02T18:11:14.611+0100 I CONTROL [main] Automatically disabling TLS 1.0, to force-enable TLS 1.0 specify --sslDisabledProtocols 'none'
2021-07-02T18:11:14.614+0100 W ASIO [main] No TransportLayer configured during NetworkInterface startup
2021-07-02T18:11:14.615+0100 I CONTROL [initandlisten] MongoDB starting : pid=332183 port=27017 dbpath=/data/db 64-bit host=kali
2021-07-02T18:11:14.615+0100 I CONTROL [initandlisten] db version v4.2.14
2021-07-02T18:11:14.615+0100 I CONTROL [initandlisten] git version: 0e6db36e92d82cc81cbd40ffd607eae88dc1f09d
2021-07-02T18:11:14.615+0100 I CONTROL [initandlisten] OpenSSL version: OpenSSL 1.1.1k 25 Mar 2021
2021-07-02T18:11:14.615+0100 I CONTROL [initandlisten] allocator: tcmalloc
2021-07-02T18:11:14.615+0100 I CONTROL [initandlisten] modules: none
2021-07-02T18:11:14.616+0100 I CONTROL [initandlisten] build environment:
2021-07-02T18:11:14.616+0100 I CONTROL [initandlisten] distmod: debian10
2021-07-02T18:11:14.616+0100 I CONTROL [initandlisten] distarch: x86_64
2021-07-02T18:11:14.616+0100 I CONTROL [initandlisten] target_arch: x86_64
2021-07-02T18:11:14.616+0100 I CONTROL [initandlisten] options: { net: { bindIp: "127.0.0.1" }, security: { authorization: "enabled" }, storage: { dbPath: "/data/d
2021-07-02T18:11:14.617+0100 W STORAGE [initandlisten] Detected unclean shutdown - /data/db/mongod.lock is not empty.
2021-07-02T18:11:14.617+0100 I STORAGE [initandlisten] Detected data files in /data/db created by the 'wiredTiger' storage engine, so setting the active storage en
2021-07-02T18:11:14.617+0100 W STORAGE [initandlisten] Recovering data from the last clean checkpoint.
2021-07-02T18:11:14.617+0100 I STORAGE [initandlisten]
2021-07-02T18:11:14.617+0100 I STORAGE [initandlisten] ** WARNING: Using the XFS filesystem is strongly recommended with the WiredTiger storage engine
2021-07-02T18:11:14.617+0100 I STORAGE [initandlisten] ** See http://dochub.mongodb.org/core/prodnotes-filesystem
2021-07-02T18:11:14.617+0100 I STORAGE [initandlisten] wiredtiger_open config: create,cache_size=561M,cache_overflow=(file_max=0M),session_max=33000,eviction=(thre
2021-07-02T18:11:14.617+0100 I STORAGE [initandlisten] stics=(fast),log=(enabled=true,archive=true,path=journal,compressor=snappy),file_manager=(close_idle_time=100000,close_scan_interval=10,close_handle_minimum=250),s
2021-07-02T18:11:14.617+0100 I STORAGE [initandlisten] ree_checkpoint_progress=
```

Рисунок 5. Результат команды

С помощью команды `mongo` мы открываем СУБД для редактирования БД (рис. 6). Например, команда `show dbs` показывает имеющиеся БД.

```
(root@kali)~[~/var/www/html/test]
└─# mongo
MongoDB shell version v4.2.14
connecting to: mongodb://127.0.0.1:27017/?compressors=disabled&gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("657618d8-20cb-4bcf-9de2-6de8c599e622") }
MongoDB server version: 4.2.14
Server has startup warnings:
2021-07-02T18:16:43.476+0100 I STORAGE [initandlisten]
2021-07-02T18:16:43.476+0100 I STORAGE [initandlisten] ** WARNING: Using the XFS filesystem is strongly recommended with the WiredTiger storage engine
2021-07-02T18:16:43.476+0100 I STORAGE [initandlisten] ** See http://dochub.mongodb.org/core/prodnotes-filesystem
2021-07-02T18:16:44.515+0100 I CONTROL [initandlisten]
2021-07-02T18:16:44.515+0100 I CONTROL [initandlisten] ** WARNING: Access control is not enabled for the database.
2021-07-02T18:16:44.515+0100 I CONTROL [initandlisten] ** Read and write access to data and configuration is unrestricted.
2021-07-02T18:16:44.515+0100 I CONTROL [initandlisten] ** WARNING: You are running this process as the root user, which is not recommended.
2021-07-02T18:16:44.516+0100 I CONTROL [initandlisten]
2021-07-02T18:16:44.516+0100 I CONTROL [initandlisten]
2021-07-02T18:16:44.516+0100 I CONTROL [initandlisten] ** WARNING: /sys/kernel/mm/transparent_hugepage/enabled is 'always'.
2021-07-02T18:16:44.516+0100 I CONTROL [initandlisten] ** We suggest setting it to 'never'
2021-07-02T18:16:44.516+0100 I CONTROL [initandlisten]
---
Enable MongoDB's free cloud-based monitoring service, which will then receive and display
metrics about your deployment (disk utilization, CPU, operation statistics, etc).

The monitoring data will be available on a MongoDB website with a unique URL accessible to you
and anyone you share the URL with. MongoDB may use this information to make product
improvements and to suggest MongoDB products and deployment options to you.

To enable free monitoring, run the following command: db.enableFreeMonitoring()
To permanently disable this reminder, run the following command: db.disableFreeMonitoring()
---
> show dbs
admin 0.000GB
config 0.000GB
database 0.000GB
local 0.000GB
user 0.000GB
>|
```

Рисунок 6. Результат команды `mongo`

После добавления пользователей, некоторые из них представлены на рисунке 7, нами был написан PHP скрипт для подключения к БД (рис.8).

```

> use admin
switched to db admin
> show users
{
  "_id" : "admin.Admin",
  "userId" : UUID("548f53a4-e1cf-4737-9a1a-17c6957898f8"),
  "user" : "Admin",
  "db" : "admin",
  "roles" : [
    {
      "role" : "userAdminAnyDatabase",
      "db" : "admin"
    },
    {
      "role" : "readWriteAnyDatabase",
      "db" : "admin"
    }
  ],
  "mechanisms" : [
    "SCRAM-SHA-1",
    "SCRAM-SHA-256"
  ]
}
{
  "_id" : "admin.Jonn",
  "userId" : UUID("07e5ac7d-c80d-488d-b240-e898b6985cb7"),
  "user" : "Jonn",
  "db" : "admin",
  "roles" : [
    {
      "role" : "readWrite",
      "db" : "admin"
    }
  ],
  "mechanisms" : [
    "SCRAM-SHA-1",
    "SCRAM-SHA-256"
  ]
}
}

```

Рисунок 7. Пользователи базы данных admin

Скрипт записывает подключения всех пользователей. Если зашел пользователь Admin, то он выводит журнал посещения (рис. 9).

```

<?php
    if ( isset($_GET["user"]) and isset($_GET["password"]) )
    {
        $usr = $_GET["user"];

        $psw = $_GET["password"] ;
        $auth=$usr. ":" . $psw;
        require 'vendor/autoload.php'; // include Composer's autoloader

        $conn = new MongoClient("mongodb://" . $auth . "@localhost:27017");

        $collection = $conn->database->coll1;
        date_default_timezone_set('UTC');
        $result = $collection->insertOne( [ 'name' => $usr, 'data'=>date(DATE_RFC822) ] );
        $col= $conn->database->coll1;

        $cursor=$col->find();
        foreach($cursor as $obj){
            if($usr=='Admin'){
                echo $obj['name'] . " " . $obj['data'] . '<br/>';
            }
        }
    }
?>

<!DOCTYPE html>
<html lang="en">
    <head>
        <title>Shop login</title>
    </head>
    <body>
        <form action="" method="GET" class="form-signin">
            <h2>Please login</h2>
            <label for="user" class="sr-only">Username</label>
            <input type="text" name="user" id="user" class="form-control" placeholder="Username" required="" autofocus=""><br/><br/>
            <label for="password" class="sr-only">Password</label>
            <input type="password" id="password" name="password" class="form-control" placeholder="Password" required=""><br/><br/>
            <button class="btn btn-lg btn-primary btn-block" type="submit">Log in</button>
        </form>
    </body>

```

Рисунок 8. Скрипт

```
Admin Fri, 02 Jul 21 11:00:32 +0000
Admin Fri, 02 Jul 21 11:02:20 +0000
Jonn Fri, 02 Jul 21 11:04:25 +0000
Admin Fri, 02 Jul 21 11:15:48 +0000
Admin Fri, 02 Jul 21 11:18:13 +0000
admin Fri, 02 Jul 21 11:19:08 +0000
Admin Fri, 02 Jul 21 11:19:44 +0000
Admin Fri, 02 Jul 21 11:20:08 +0000
Admin Fri, 02 Jul 21 11:20:49 +0000
Admin Fri, 02 Jul 21 11:22:32 +0000
Admin Fri, 02 Jul 21 11:22:47 +0000
Admin Fri, 02 Jul 21 11:23:50 +0000
Admin Fri, 02 Jul 21 11:59:03 +0000
admin Fri, 02 Jul 21 11:59:12 +0000
Admin Fri, 02 Jul 21 12:01:30 +0000
Admin Fri, 02 Jul 21 12:02:29 +0000
Admin Fri, 02 Jul 21 12:03:19 +0000
admin Fri, 02 Jul 21 12:10:54 +0000
admin Fri, 02 Jul 21 12:13:09 +0000
Admin Fri, 02 Jul 21 13:45:28 +0000
admin Fri, 02 Jul 21 14:07:15 +0000
admin Fri, 02 Jul 21 14:07:30 +0000
admin Fri, 02 Jul 21 14:07:30 +0000
admin Fri, 02 Jul 21 14:08:48 +0000
admin Fri, 02 Jul 21 14:08:49 +0000
Admin Fri, 02 Jul 21 15:03:04 +0000
```

Please login

Username

Password

Рисунок 9. Результат подключения пользователя Admin

ЗАКЛЮЧЕНИЕ

В ходе проделанной работы мы ознакомились с NoSQL, на примере MongoDB, а также с NoSQLMap; написали скрипт подключения и редактирования базы данных.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. SQL и NoSQL инъекции [Электронный ресурс] – URL: <https://cisoclub.ru/sql-i-nosql-inekczii-podrobnyj-razbor-i-analiz/> (дата обращения: 1.07.2021)
2. MongoDB [Электронный ресурс] – URL: <https://ru.wikipedia.org/wiki/MongoDB> (дата обращения: 1.07.2021)
3. Setup MongoDB in Kali Linux [Электронный ресурс] – URL: <https://medium.com/cyber4people/setup-mongodb-in-kali-linux-3ab86731e3ec> (дата обращения: 1.07.2021)
4. Using the PHP Library for MongoDB (PHPLIB) [Электронный ресурс] – URL: <https://www.php.net/manual/en/mongodb.tutorial.library.php> (дата обращения: 1.07.2021)
5. NoSQLMap [Электронный ресурс] – URL: <https://kali.tools/?p=1259> (дата обращения: 1.07.2021)
6. NoSQLMap [Электронный ресурс] – URL: <https://materials.rangeforce.com/tutorial/2019/05/13/NoSQLMap/> (дата обращения: 1.07.2021)