ÁMBITO Y ALCANCE DE LA AUDITORÍA

La auditoría se ha realizado en Kali Linux, utilizando la herramienta Nmap, se han recuperado los siguientes datos sobre puertos, SO y lenguaje utilizado:

Escaneando la IP http://127.0.0.1 con nmap lanza estos resultados:

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-06 10:47 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00022s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
8080/tcp  open  http-proxy
9090/tcp  open  zeus-admin
42525/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds
```

puertos abiertos: 8080, 9090 y 42525

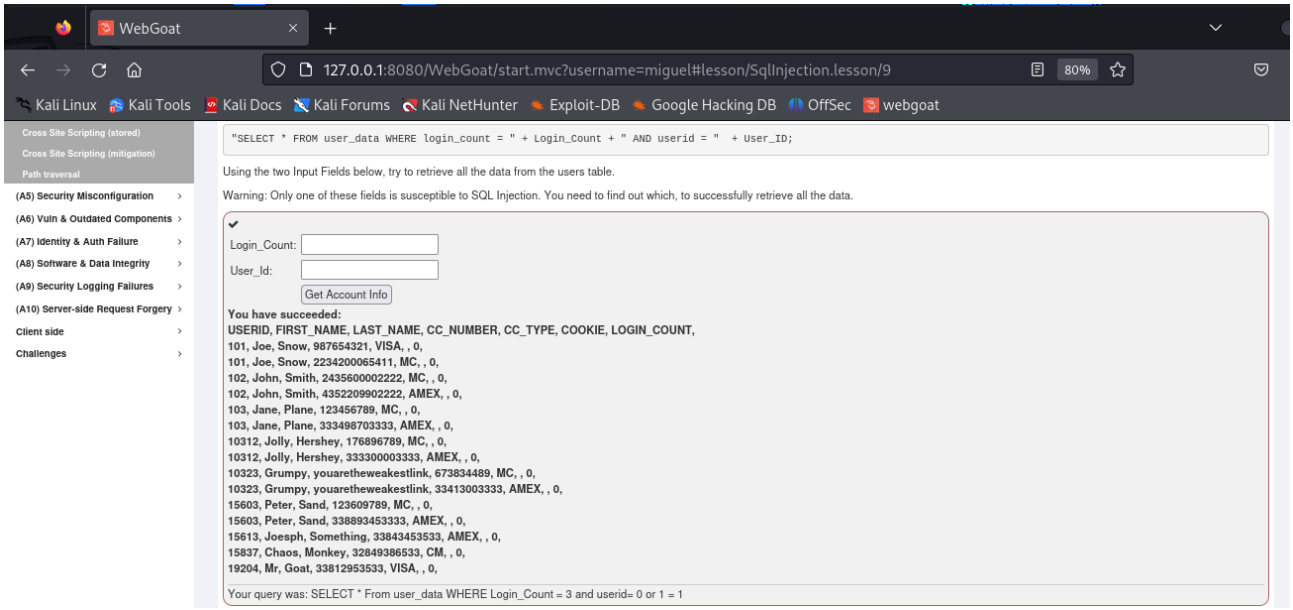
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 127.0.0.1
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-06 11:05 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00012s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
8080/tcp open  http-proxy
9090/tcp open  zeus-admin
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

la aplicación WebGoat está creada en java 21

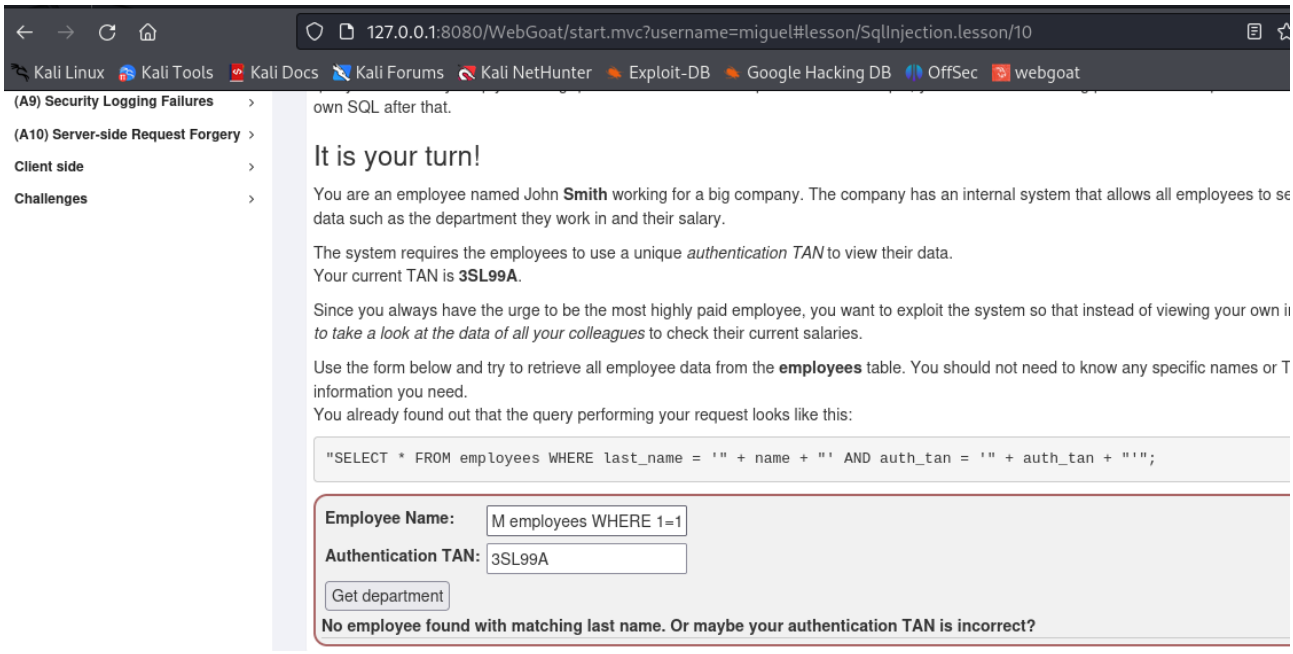
```
┌──(kali㉿kali)-[/home/kali]
└─PS> sudo docker run -it -p 127.0.0.1:8080:8080 -p 127.0.0.1:9090:9090 -e TZ=Europe/Berlin webgoat/webgoat
[sudo] password for kali:
2023-12-07T15:36:32.956+01:00  INFO 1 --- [           main] org.owasp.webgoat.server.StartWebGoat    : Starting StartWebGoat v2023.8 using Java 21.0.1 with PID 1 (
me/webgoat/webgoat.jar started by webgoat in /home/webgoat)
```

La auditoría se ha realizado en Kali Linux, explotando las siguientes vulnerabilidades:

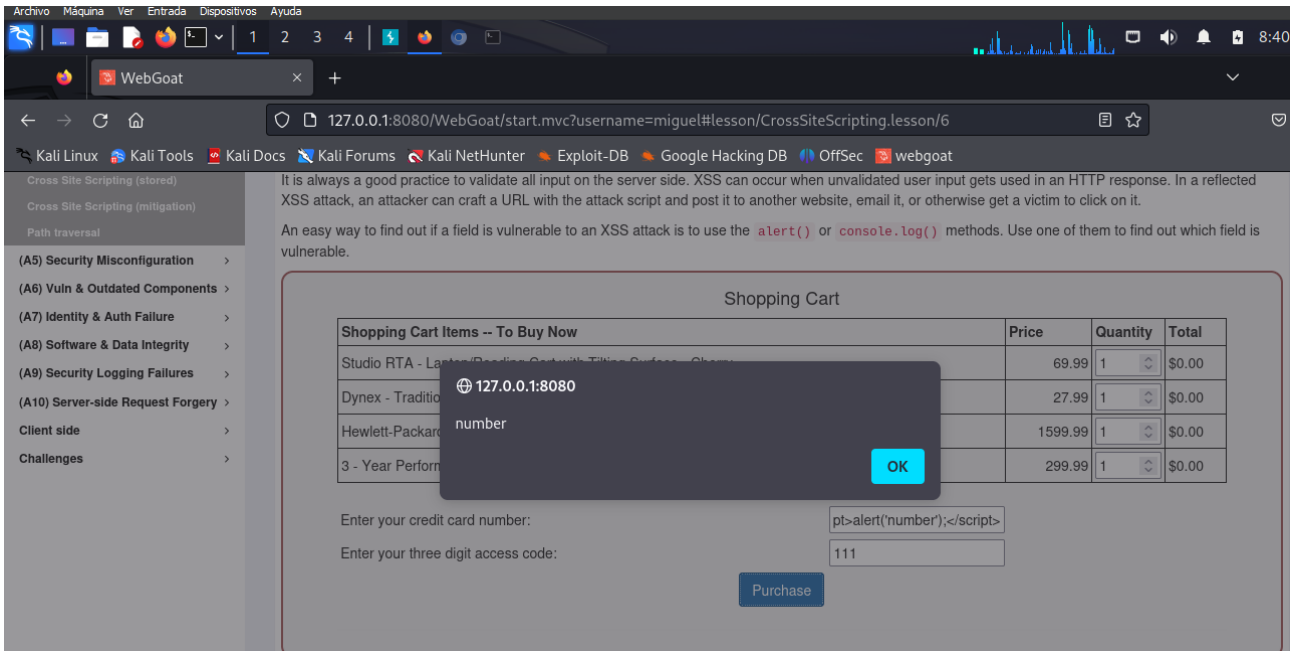
A3 Injection - SQL Injection (intro) - Apartado 10

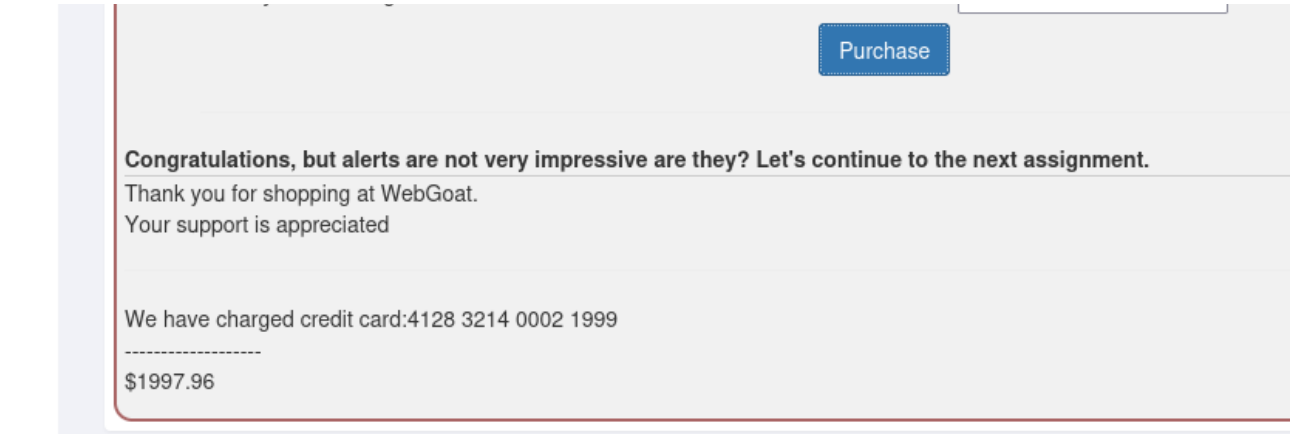



A3 Injection - SQL Injection (intro) - Apartado 11

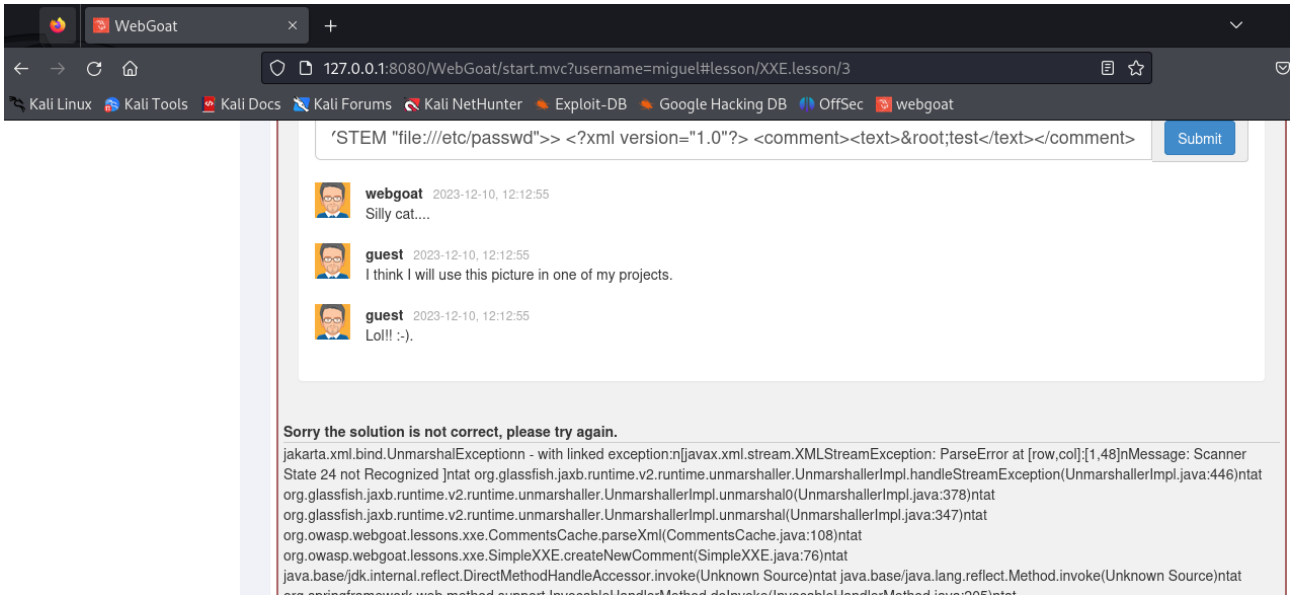



A3 Injection - Cross Site Scripting - Apartado - Apartado 7

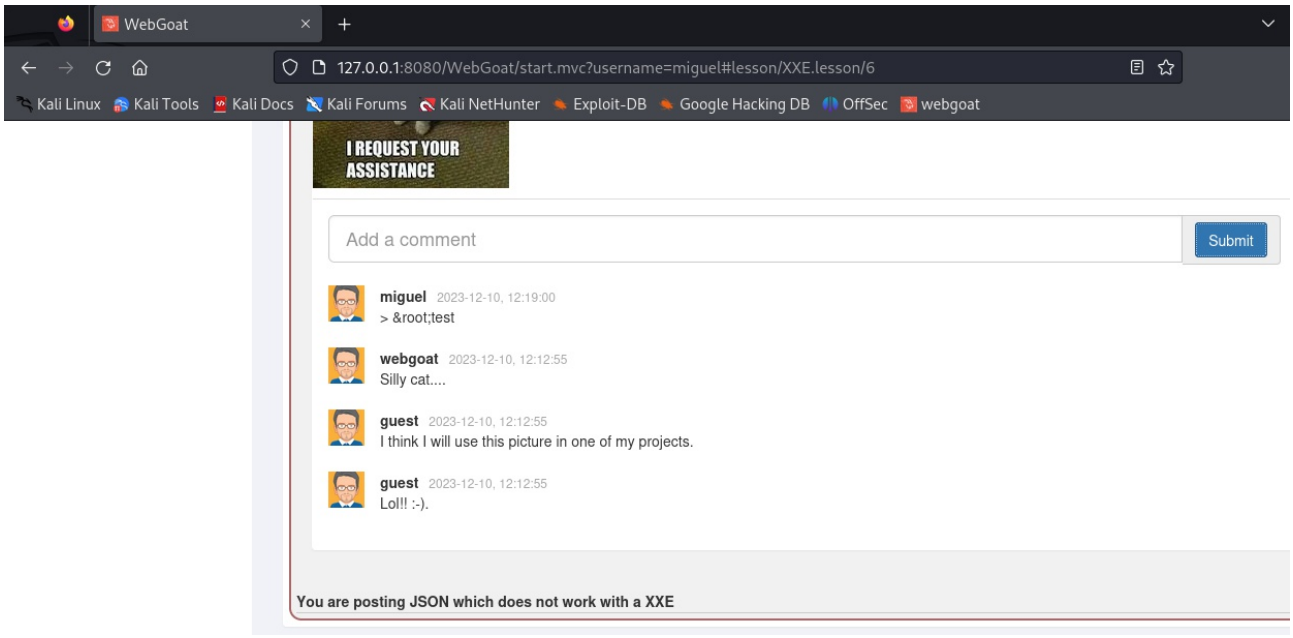


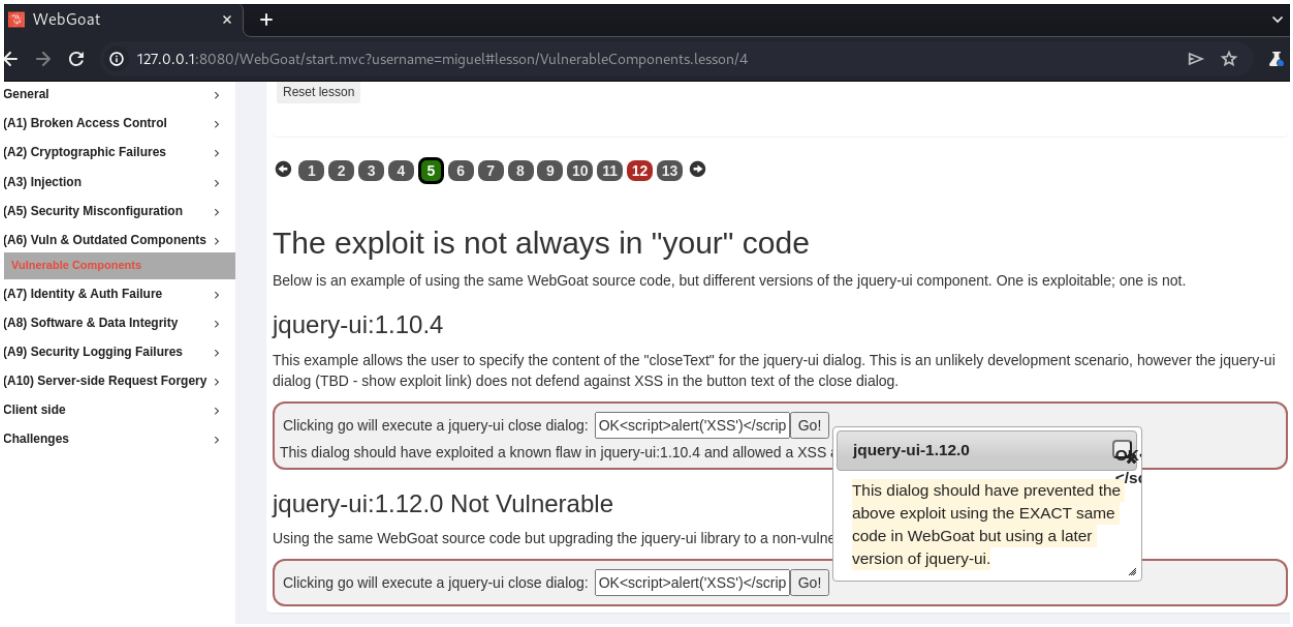

A5 Security Misconfiguration - Apartado 4



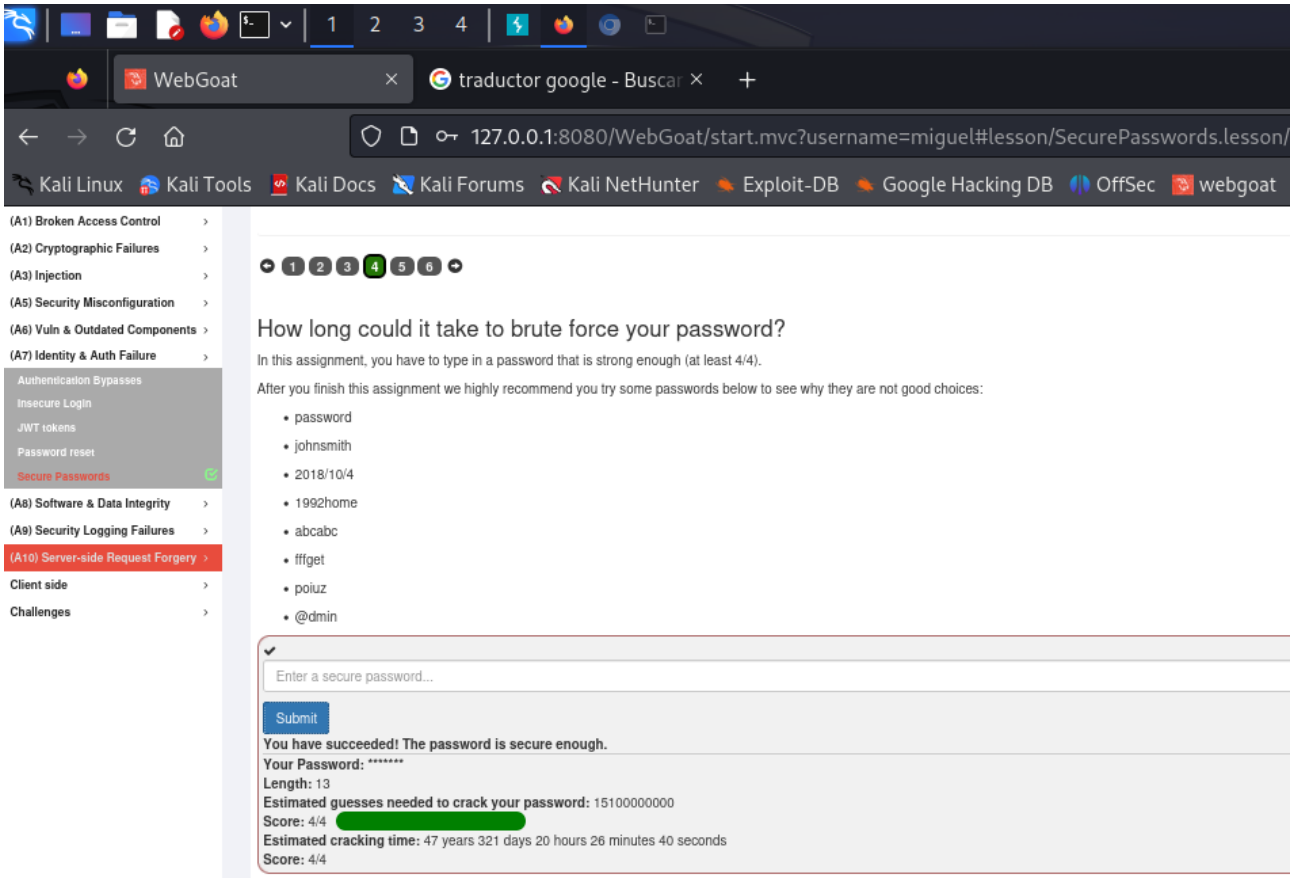
A5 Security Misconfiguration - Apartado 7




A6 Vuln & outdated Components - Apartado 5




A7 Identity & Auth Failure - Secure Passwords Apartado 4


1 2 3 4
WebGoat
traductor google - Buscar
127.0.0.1:8080/WebGoat/start.mvc?username=miguel#lesson/SecurePasswords.lesson/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
webgoat
(A1) Broken Access Control
(A2) Cryptographic Failures
(A3) Injection
(A5) Security Misconfiguration
(A6) Vuln & Outdated Components
(A7) Identity & Auth Failure
Authentication Bypasses
Insecure Login
JWT tokens
Password reset
Secure Passwords
(A8) Software & Data Integrity
(A9) Security Logging Failures
(A10) Server-side Request Forgery
Client side
Challenges
1 2 3 4 5 6
How long could it take to brute force your password?
In this assignment, you have to type in a password that is strong enough (at least 4/4).
After you finish this assignment we highly recommend you try some passwords below to see why they are not good choices:
password
johnsmith
2018/10/4
1992home
abcabc
fffget
poiuz
@dmin
Enter a secure password...
Submit
You have succeeded! The password is secure enough.
Your Password: *******
Length: 13
Estimated guesses needed to crack your password: 15100000000
Score: 4/4
Estimated cracking time: 47 years 321 days 20 hours 26 minutes 40 seconds
Score: 4/4