Sanity Checks

kindly take a seat

we have a fun challenge after the quick session on passwords

0x1337

The Hacking Club

rockyou.txt

rockyou

> started: 2005

> developed widgets

> password breach: 2009

10 year old SQLI

Unencrypted database

Passwords stored
in plain text

ALL passwords stolen

The hacker

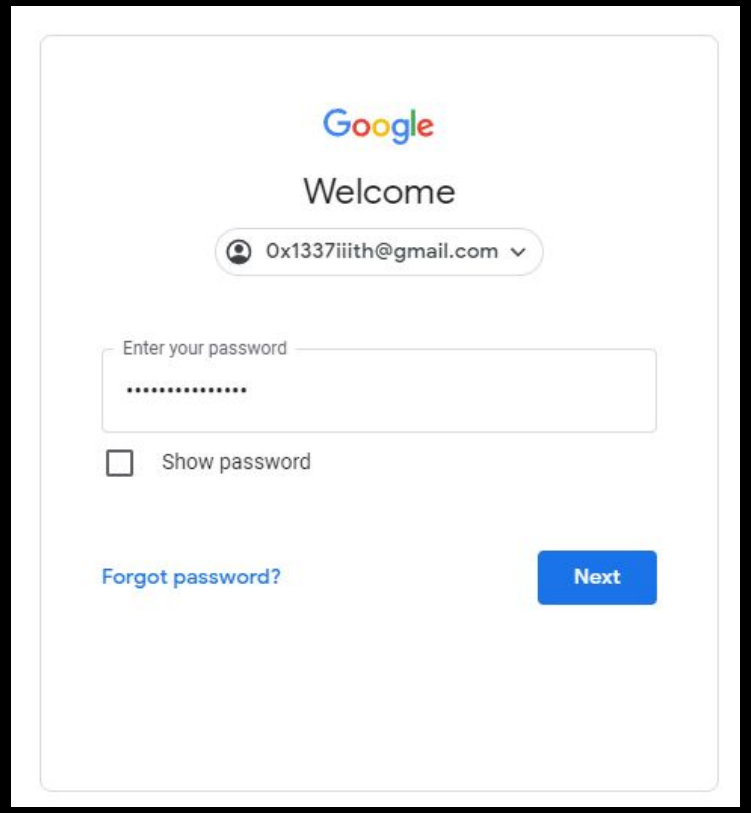
> did not ask for money

> did not sell the information on the dark web

> simply uploaded a file: rockyou.txt

Passwords

Method 0: Plain Text



Method 0: Plain Text

email	password
0x1337@gmail.com	password1234isnotstrong
narc.zuccerberg@example.com	iloveyourdata

Method 1: Encodings

password 

70617373776F7264

password 

OBQXG43XN5ZGI===

password 

cGFzc3dvcmQ=

It is easy to go both the directions

Method 1: Encodings

password 

70617373776F7264

password 

OBQXG43XN5ZGI===

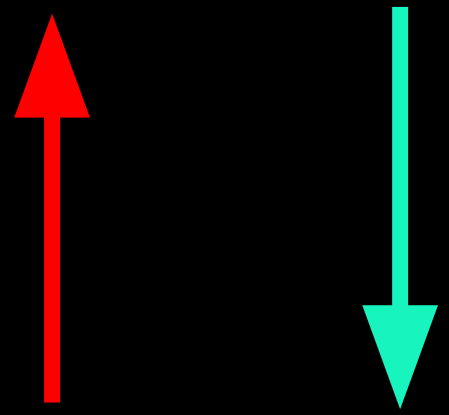
password 

cGFzc3dvcmQ=

A one way function?

Method 2: Hashing

password



5f4dcc3b5aa765d61d8327deb882cf99

Method 2: Hashing

> currently the best way to store passwords

> some popular ones:

  > MD 2/5

  > SHA 1/2/3

So, we are done, right?

Remember rockyou.txt?

123456789
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
password
michael
qwerty
...

5f4dcc3b5aa765d61d8327deb882cf99

Hello, agent 008,
A recent investigation into the Evil Corporation Beta revealed they use a static IV for their AES CBC encrypted data. We sent agent 001's team to exploit this vulnerability.

Before we give you the main task, we need to ensure you are fit for the job. You need to go to their under-construction website and crack the passwords of their low-level employees.

the link to the challenge is on our linktree (beta challenge)
https://linktr.ee/0x1337

---

upload the solutions to (need to be on college lan)
http://10.4.16.150

Methods: Summary

- common encodings:
  - base 16/32/64
  - can be broken using decoders
- common hash functions:
  - MD 2/5
  - SHA 1/2/3
  - can be broken using bruteforce: “hash cracking”

Congratulations! You have proven your skills. Here is what you need to know.

While deep undercover, agent 001 and his team used the vulnerability in the **AES CBC encryption** to identify their **secret key**, and **IV** are both **'thisismypassword'**. 001 created a backdoor in the website and transmitted us this intel. Unfortunately, 001 was captured by the **Beta** Minions right after the transmission.

Your mission is to use this intel to crack the password of the CEO of Beta. 001's life depends on you.