Welcome to the CoGrammar

Hashing Over the web

The session will start shortly...

Questions? Drop them in the chat. We'll have dedicated moderators answering questions.

CoGrammar

Cyber Security Session Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly. **(Fundamental British Values: Mutual Respect and Tolerance)**
- No question is daft or silly - **ask them!**
- There are **Q&A sessions** midway and at the end of the session, should you wish to ask any follow-up questions.
- If you have any questions outside of this lecture, or that are not answered during this lecture, please do submit these for upcoming Academic Sessions. You can submit these questions here: **Questions**

Cyber Security Session Housekeeping cont.

- For all **non-academic questions**, please submit a query: www.hyperiondev.com/support
- We would love your **feedback** on lectures: [Feedback on Lectures]
- Find all the lecture **content** in you [Lecture Backpack] on GitHub.
- If you are hearing impaired, please kindly use your computer's function through Google chrome to enable captions.

Safeguarding & Welfare

We are committed to all our students and staff feeling safe and happy; we want to make sure there is always someone you can turn to if you are worried about anything.

If you are feeling upset or unsafe, are worried about a friend, student or family member, or you feel like something isn't right, speak to our safeguarding team:

Ian Wyles
Designated Safeguarding Lead

Simone Botes

Nurhaan Snyman

Rafiq Manan

Ronald Munodawafa

Tevin Pitts

Scan to report a safeguarding concern

or email the Designated Safeguarding Lead:
Ian Wyles
safeguarding@hyperiondev.com

CoGrammar HyperionDev

Stay Safe Series:

Mastering Online Safety One week at a Time

While the digital world can be a wonderful place to make education and learning accessible to all, it is unfortunately also a space where harmful threats like online radicalization, extremist propaganda, phishing scams, online blackmail and hackers can flourish.

As a component of this BootCamp the *Stay Safe Series* will guide you through essential measures in order to protect yourself & your community from online dangers, whether they target your privacy, personal information or even attempt to manipulate your beliefs.

Security Tip

Limit user permissions to the minimum required for their roles. By applying the principle of least privilege, you reduce the risk of unauthorized access or accidental data exposure, even if a breach occurs."

SKILLS FOR LIFE
SKILLS BOOTCAMPS

Department for Education

CoGrammar

Hashing Over the Web

November 2024

Learning Objectives & Outcomes

- Define hashing and its purpose in data security
- Differentiate between hashing and encryption, focusing on their purposes, reversibility, and key management.
- Propose preventive measures to mitigate brute force attacks, such as salting, two-factor authentication, and password complexity policies.
- Identify brute force attacks and tools in Kali Linux, such as Hydra and John the Ripper.

CoGrammar

Data Security

- Have you ever wondered how websites keep your passwords secure so that even if someone steals them, they can't easily figure out what they are?

CoGrammar

Polls

Please have a look at the poll notification and select an option.

What do you think happens to your password when you enter it on a secure website?

A. It's stored as you entered it
B. It's encrypted
C. It's hashed
D. I'm not sure

CoGrammar

Polls

Please have a look at the poll notification and select an option.

What do you think is harder to break: a hashed password or an encrypted password?

A. Hashed password
B. Encrypted password
C. Both are equally hard
D. I'm not sure

CoGrammar

Hashing and Encryption in CyberSecurity

- **Importance of Data Security:**
  - SafeGuarding sensitive data against misuse and abuse
- **Key Techniques:**
  - Hashing
  - Encryption
- **Applications:**
  - Password security
  - Digital Signatures
  - Data retrieval

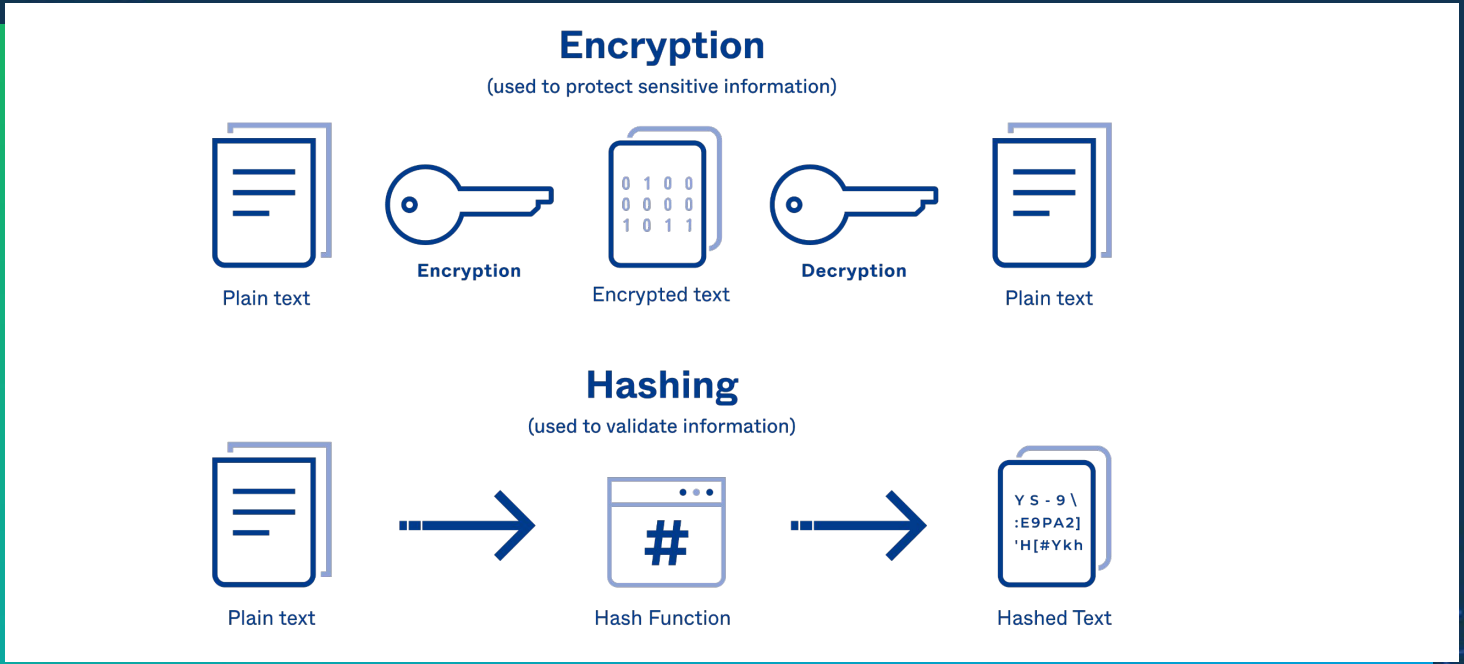
CoGrammar

Hashing vs Encryption

Aspect	Hashing	Encryption
Purpose	Creates unique data representations	Protects data confidentiality
Reversibility	One-way process, irreversible.	Two-way process; reversible with a key
Key Management	Does not require a key	Requires a secret key for encryption/decryption
Output size	Fixed output size	Output size matches input size.

CoGrammar

Hashing vs Encryption



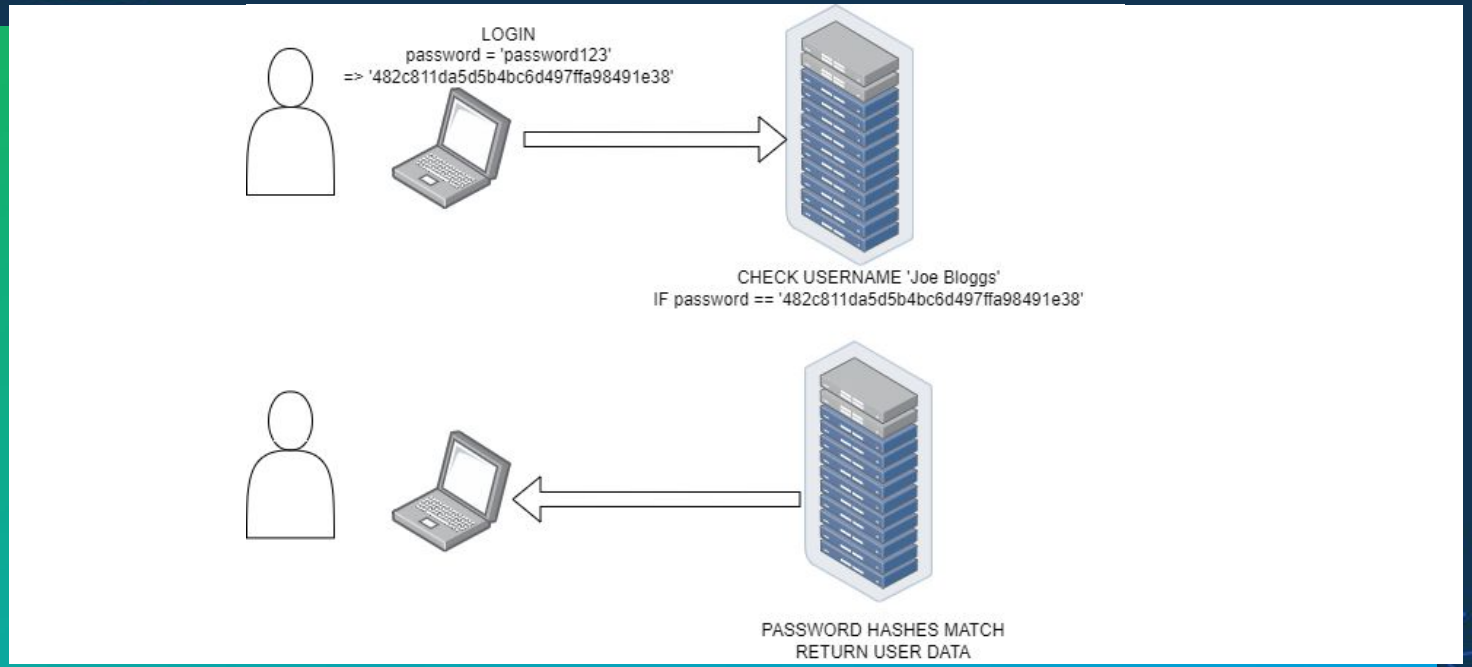
CoGrammar

Password Hashing

- **Why Hash Password?**
  - Prevents hackers from reading stolen passwords
  - Irreversible process with fixed-length hashes
- **Key properties of Hashes:**
  - Deterministic: Same input generates the same output
  - Irreversible: No hints about original data
  - Fixed-length: Input length does not affect hash size.
- **Hash Collisions:**
  - Rare but possible: When two or more unique passwords generate the same hash.

CoGrammar

Password Hashing



CoGrammar

Creating a Hash Function

index.py

```python
import hashlib


def string_hasher(input_string):
    """
    This function takes an input string, encodes it into a UTF-8 byte format,and
    applies the SHA-256 hashing algorithm to it. The result is then converted
    into a readable hexadecimal string using the hexdigest() method, which can
    be used to securely store or compare sensitive information.
    """
    hashed_string = hashlib.sha256(input_string.encode()).hexdigest()
    return hashed_string


# Call the function with the strings that we would like to hash.
hashed1 = string_hasher("This is sensitive text.")
hashed2 = string_hasher("_password-123_")

# Here we can demonstrate the result of our hashing function.
print(f"\'_password-123_\' \t-->Hash Function-->\t {hashed1}")
```

Snipped

CoGrammar

Password Cracking Techniques

- **Cracking (or hash cracking)** can technically reverse a hash. It is simply a brute-force approach to auto-generating passwords, hashing them, and checking them against all hashes.
- **Techniques:**
  - Brute Force attacks
  - Dictionary Attacks
  - Hybrid Attacks
  - Credential Stuffing

Brute Force Attacks

- **Definition**: A comprehensive attack that systematically tries every possible combination of characters to crack a password.
- **How it works:**
    - Generates all potential character combinations
    - Applies the hashing algorithm to each combination and compares it to stored hashes.
    - Success is guaranteed if enough time and computational power are available

CoGrammar

Brute Force Attacks

- **Characteristics:**
  - More effective for cracking strong or complex passwords
  - Computationally expensive and time-consuming
  - Time to crack increases exponentially with password length and complexity

CoGrammar

Dictionary Attacks

- **What is a dictionary attack?**
  - A type of brute force attack where hackers use a predefined list of commonly used words, phrases, or number combinations to guess passwords
- **How it works:**
  - Attacker creates a wordlist (dictionary) of commonly used passwords.
  - Automated tools systematically test each entry from the list against user accounts.
  - Success relies on users choosing simple or predictable passwords

Key Points for prevention

- **Strong Passwords:** Use complex, random, and unique passwords.
- **Salting and Hashing:** Add a unique salt to passwords before hashing to thwart dictionary and rainbow attacks.
- **Two-Factor Authentication (2FA):** Adds an extra layer of security beyond the password.
- **Limit Login Attempts:** Restrict repeated failed login attempts to prevent brute-force attacks.
- **Educate Users:** Awareness of phishing and social engineering tactics.

Practical Example: Using Hydra for brute force

- For this practical example, I'm going to demonstrate how to perform a brute force attack on VPS (I'm using a dummy server that I bought from contabo, the password will be changed immediately after the lecture)
- Tools used:
  - Kali linux
  - Hydra
  - Cheatsheet
    - https://github.com/frizb/Hydra-Cheatsheet

CoGrammar

Polls

Please have a look at the poll notification and select an option.

What is the main purpose of hashing in cybersecurity?

A. To store passwords securely
B. To encrypt sensitive data
C. To ensure data confidentiality
D. To protect systems from viruses

CoGrammar

Polls

Please have a look at the poll notification and select an option.

How does salting improve password security?

A. By making it easier to hash passwords
B. By adding a unique string to the password before hashing
C. By encrypting the password after hashing
D. I'm not sure

CoGrammar

Questions and Answers

CoGrammar

Thank you for attending

SKILLS FOR LIFE
SKILLS BOOTCAMPS

Department for Education

CoGrammar