42 Cyber Workshop

Mika, Fred, Mike, Frank

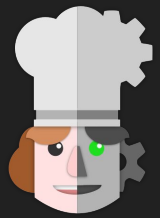
fortytwo.pwned.lu

Table of contents

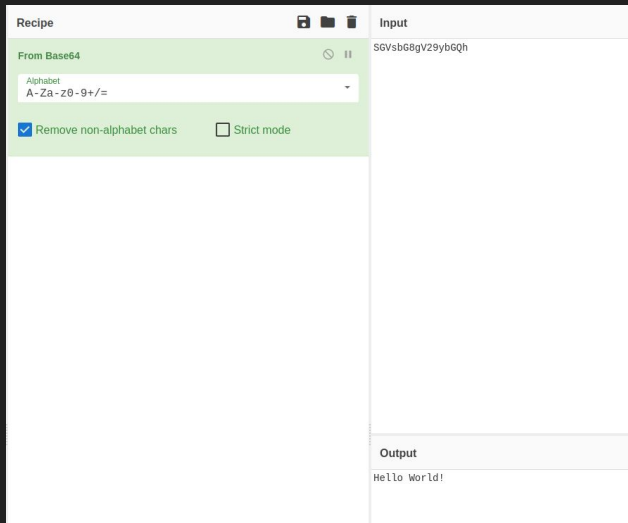
Encodings

- Representation of data
  - 13 in decimal (base 10) is 0b1101 in binary (base 2) and 0xd in hexadecimal (0-f, base 16)
- Most common:
  - Base64
  - Hex (base 16)
- Resources:
  - Cyberchef: https://gchq.github.io/CyberChef/ (Demo time)

Best tool :



CyberChef



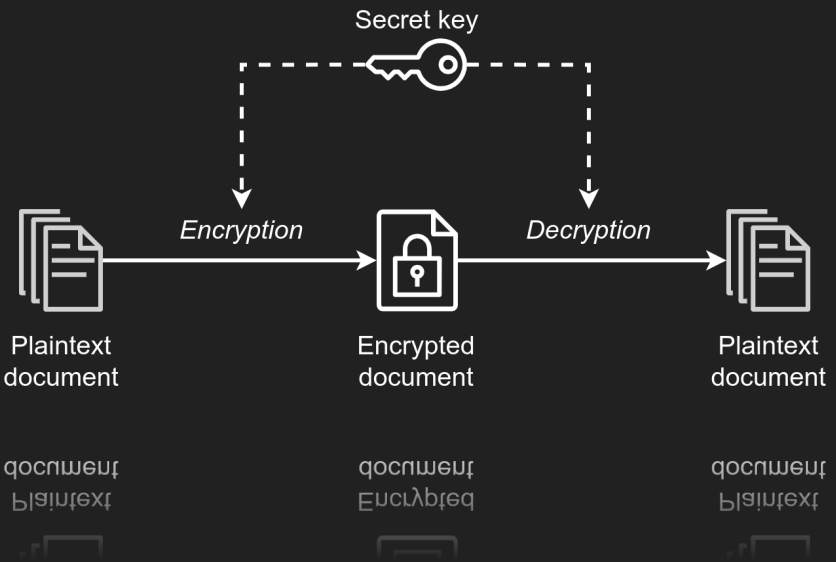
Misc - OSINT

- Open Source Intelligence
- Find information on the internet
  - google search (with google dorks, advanced search)
  - Google maps, e.g. street view
  - reverse image search
  - social media
  - metadata of public images

- Tools: https://osintframework.com/, google dorks

Crypto - Symmetric encryption

- The encryption key is the same as the decryption key
  - m = c(key)
  - m: message
  - c: ciphertext
  - key: encryption key
  - example: Caesar, xor, AES, DES

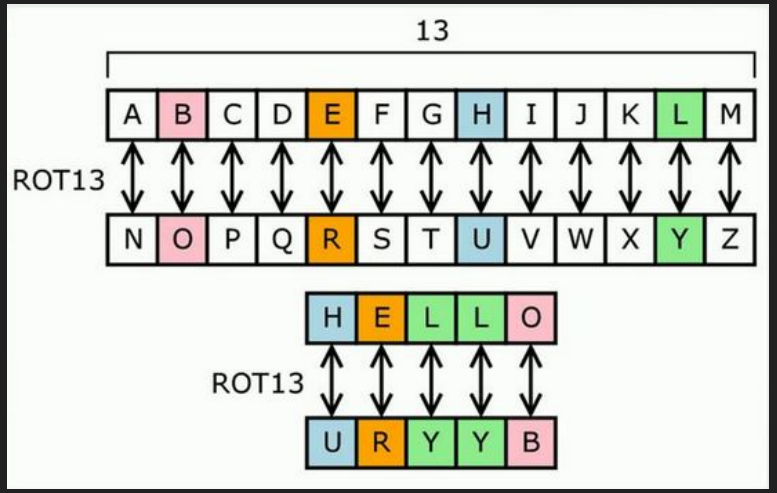


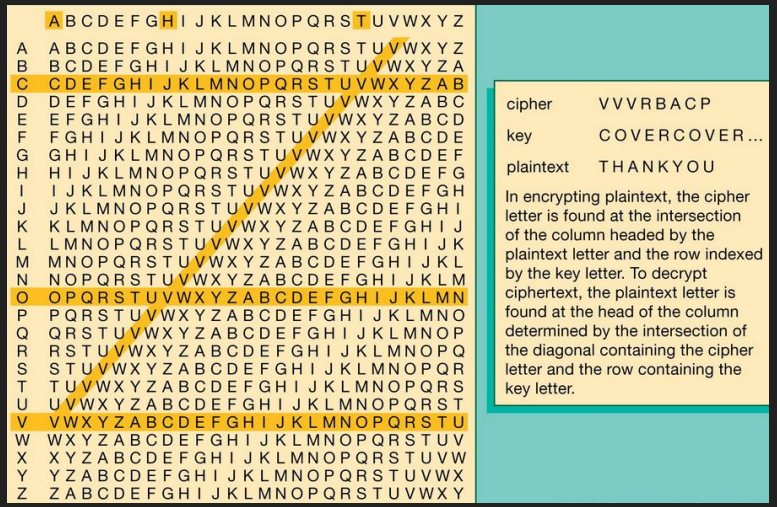
Crypto - Asymmetric encryption

- The encryption key is the same as the decryption key
  - c = pubK(m)
  - m = privK(c)
  - m: message
  - c: ciphertext
  - pubK: public key
  - privK: private key
  - Examples: RSA, ECC

Crypto - Substitution Ciphers

- Substitution Cipher
  - Caesar cipher being the most famous one
  - Can easily be cracked with frequency analysis.
  - e.g. “e” is the most common letter in English
- Vigenère Cipher
  - A substitution cipher with a password
- Resources:
  - https://www.dcode.fr/ (demo time)





Crypto - RSA (asymmetric)

- Encryption: c = m^e mod n
  - n=p*q, e public key, is usually send along the message
  - c - ciphertext
  - m - plaintext message
- Decryption: m = c^d mod n
  - d = (p-1)*(q-1) = d private key. (p and q are two large prime numbers chosen by the user)
  - n = p*q
- Security
  - The security relies that n (which is public) cannot be factored, and p and q can not be found.
  - If n is factored, p and q can be found, and d can be calculated.

Web - General

- basically everything that has to do with websites
  - websites are being used by everyone, everywhere
  - a lot of elements in web traffic can cause security issues
- most relevant protocol in web context: HTTP
  - A protocol is a set of rules on how to communicate
  - It can be compared to the rules of sentence construction in natural language
- web security = very extensive field
  - many different attack vectors and things to consider

Web - HTTP - HyperText Transfer Protocol

- Method of communication between the client (e.g. browser) and the web-server
- The Client requests, and the server answers

Example of a HTTP GET request

- Several different HTTP methods:
  - **GET**: typically to fetch resources like html or javascript resources
  - **POST**: typically to send data to the web-server, e.g. when submitting credentials or uploading a new profile picture.
  - **PUT, DELETE, OPTIONS** etc.

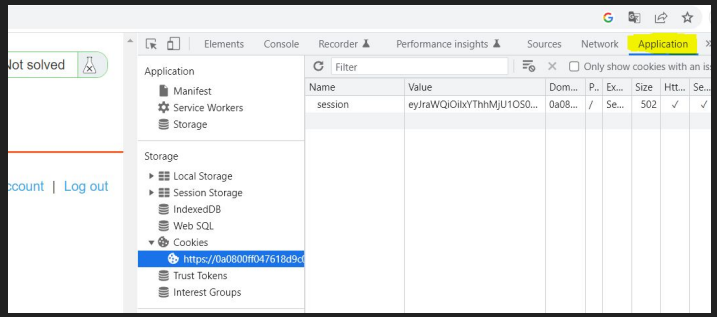
Web - Basics

- Developer tools
  - Inspector → view HTML
  - Console → interactive JS console
  - Debugger → view files
  - Network → view requests
  - Style Editor → view CSS
  - Storage → Cookies

  Demo time :)

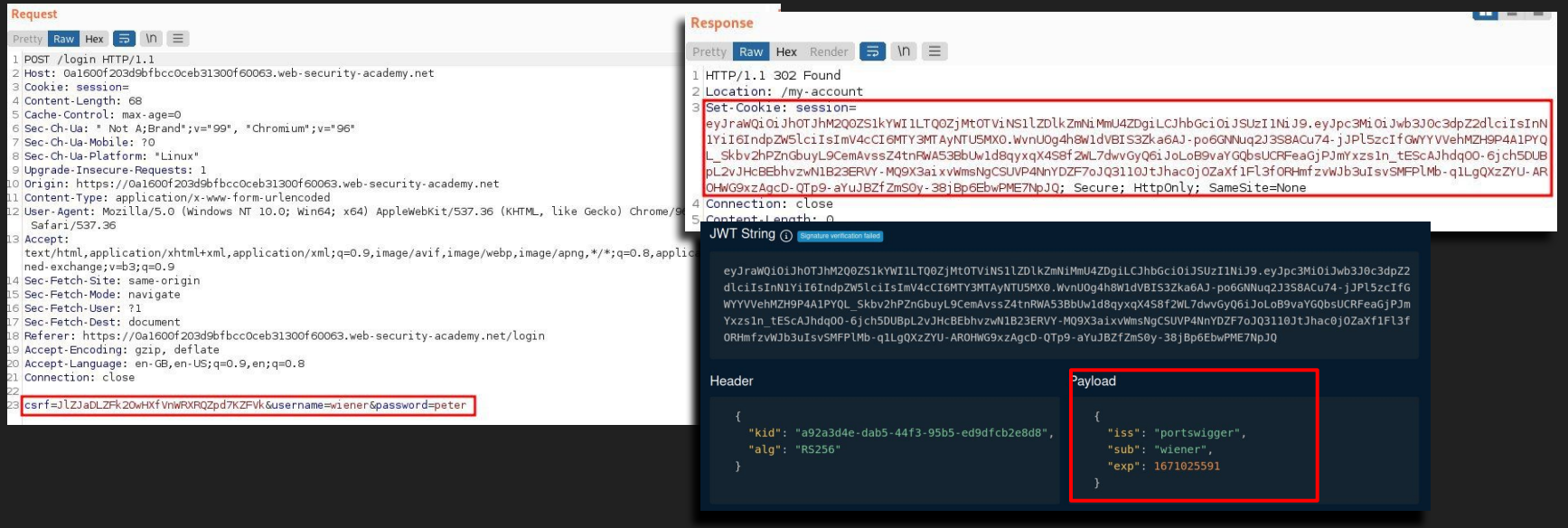
Web - Cookies

- to keep track of user sessions
- if someone logs in, they receive a cookie in the response
    - every subsequent request of the user with that cookie is recognized as logged in



Web - Cookies: JSON Web Tokens

- Structure of JWTs: (1) Header, (2) Payload, (3) Signature
- Many potential weaknesses in implementation of JWTs
- Resources: jwt.io



Web - SQL Injection

Using apostrophes (‘), quotation marks (“) or backslashes (\) to break out of a string and manipulate the actual SQL.

abc’ UNION SELECT username, password FROM users; --

Website

SELECT name, type FROM products WHERE name = ‘**$userInput**’;

Database

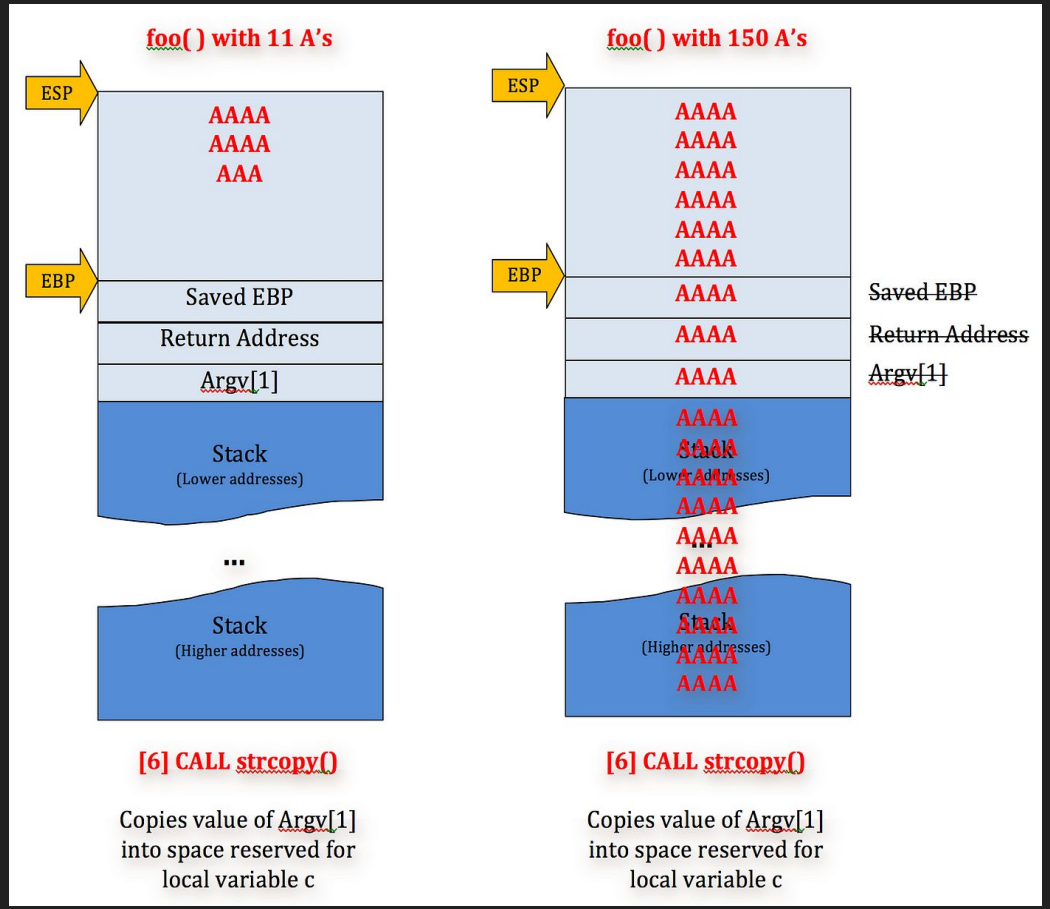
Select name, type FROM products WHERE name = ‘abc’ UNION SELECT username, password FROM users; -- ’;

Web - XSS - Cross-Site Scripting

- Client-side code injection
  - Execute code (javascript) in the browser of the victim.
  - Goal: Steal cookie, or session of the victim
- Stored XSS
  - An attacker is able to inject javascript through e.g. a comment in a forum. The text is persistent.
- Reflected XSS:
  - An attacker is able to inject javascript through a volatile method. E.g. through a HTTP parameter. The attacker has to send a link to a victim in order to exploit him

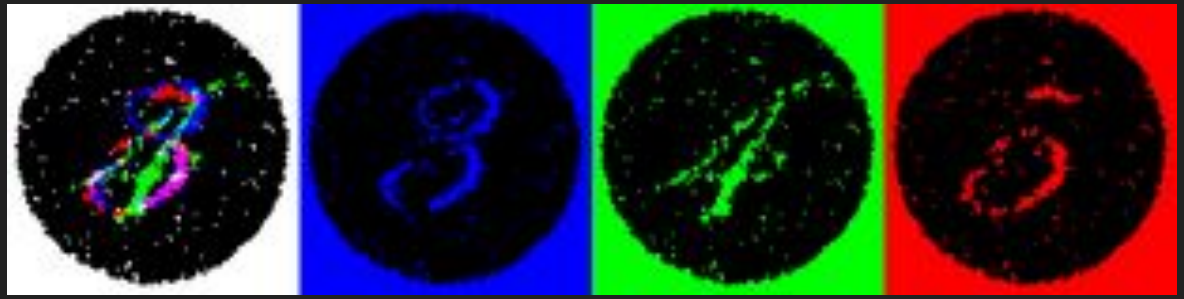
Pwn - Buffer Overflow

- Out of buffer range write
- Able to overwrite values on the stack
- Integrity of the stack gets corrupted and variables can be overwritten.
- More advanced attacks can be used to execute arbitrary code.



Misc - Steganography

- Hiding things in images
  - Metadata (e.g. time the image was created, author, size etc.)
  - Actual image (The actual pixel values)



Misc - Password cracking

- Try every combination (Brute force)
  - e.g. try 000 - 999 for a 3-digit code
  - Takes time
  - Trying all possible combinations increases exponentially with password length

- Can be done with password list - called a dictionary attack
  - Instead of all possible combinations, try the most likely ones.
  - Try weak passwords first, e.g. admin, password. 12345, 123456 …
  - Create custom dictionaries by e.g. crawling the website and compose them yourself.
  - Tools: cewl, crunch

Misc - Brute Forcing

- Online attacks
  - Launch the attack on an website or program itself
  - Tools: hydra, crackmapexec
- Offline
  - Extract the hash or a token that lets you crack the password independently of the application
  - john the ripper, hashcat

Good luck!

Want more of this?

- hack.lu is happening at the moment!
- Join our discord server (discord.letzpwn.lu)
  - Play CTFs together
  - Currently playing: hack.lu CTF
- Qualifier LCSC CTF from 1st of February-31st of March
  - For more info follow us on linkedin, twitter or X (@letzpwnasbl)