UNIVERSITY OF LIVERPOOL

CYBER SECURITY SOCIETY

~$whoarewe

```
"CyberSoc": [
   {
        "Harlan"    : "President",
        "Matthew" : "Treasurer",
        "Tom"        : "Secretary",
        "You??" :  “(Self-register on guild website 03/10/22 - 19/10/22)”
   }
],
"Structure": [
   {
        "Mission" :  "Aiding you in improving your confidence
                      towards cyber security through participating
                      in internal / external CTFs with the society  "

        "Events" :    "Meetings"
   }                  "In person internal CyberSoc CTFs"
]                     "External CTFs with organisations"
                      "Industry Talks"
                      "Group Based Challenges"
```

UNIVERSITY OF LIVERPOOL
CYBER SECURITY SOCIETY
cybersoc.cf/discord

```
import java.sql.*;
import java.awt.*;

/**
 *
 * @author jeff
 */
public class Main {

    public static String AppName = "SQL Mail";
    public static String AppVersion = " 0.0.1 ";
    public static String AppAuthor = "Jeffrey Cobb";
    public static String AppDate = "August 8th, 2007";
    public static String AppPath = System.getProperty("user.dir");
    public static String AppDriver = "smallsql.database.SSDriver";
    public static String AppDBHeader = "jdbc:smallsql:";
    public static String AppDBPath = AppPath + "/sqlmail";
    public static String AppPreferences = AppPath + "/sqlmail_prefs";
    /** Creates a new instance of Main */
    public Main() {
    }

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) throws Exception {
        // TODO code application logic here

        boolean bDBConnect = false;
        int result = 0;
        frmMain SQLMailForm = new frmMain();
        System.out.println("\r\n" + AppName + "\r\nVersion" + AppVersion + "\r\nAuthor: " + AppAuthor +
-- " + AppDate + "\r\n");

        Toolkit tk = Toolkit.getDefaultToolkit();
        Dimension screen = tk.getScreenSize();
        System.out.println(screen.getWidth() + " --- " + screen.getHeight());
```

~$what_is_linux

```
"Linux": [
   {
        "Distros" :  "Operating system made from a software
                      collection that includes the Linux kernel
                      and, often, a package management
                      system"
        "Virtual Machines" :  "Virtualization/emulation of a
                               computer architectures and provide
                               functionality of a physical computer"
   }
],
"Kali Linux": [
   {
        "What " :   "Open-source, Debian-based Linux
                     distribution aimed at advanced
                     Penetration Testing and Security"
        "Purpose" :  "Feature Rich with security analysis,
                      security auditing, and penetration testing
                      tools"
   }
]
```

~$what_is_hacking

```
"Hacking": [
    {
        "Definition" : "Gaining of unauthorized access to data in a system or computer"
        "Types" : { "White Hat" , "Black Hat" }
        "Industry" : {"Red Team" , "Blue Team"}
    }
],

"Inspect Element": [
    {
        "Use" : "Find hidden code elements in websites that may be commented out"
        "Tools" : "Developer Console"
    }
],
```

```
"Port Scanning": [
    {
        "Use" : "Find open ports on servers that could be exploited"
        "Tools" : "Nmap"
    }
],
"Web Content Scanner": [
    {
        "Use" : "Find hidden url paths or subdomains connected to a website"
        "Tools" : "Gobuster / wfuzz / dirb"
    }
],
"Hash Cracking": [
    {
        "Use" : "Crack hashes to reveal data received"
        "Tools" : "John the Ripper"
    }
]
```

~$what_is_inspect_element

```
"What is it": [
    {
        "Inspect Element is a useful developer tool that can be easily exploited for
        many different purposes"
        "Inspector" : "Scroll through the source code to find hidden elements"
        "Console" : "Inject Javascript into the site to exploit functions (XSS)"
        "Network" : "See all GET & POST requests to and from the server (replay attacks)"
        "Storage" : "View all variables within a site can be used (cookie hijacking)"
    }
],
"Format": [
    {
        "Developer Tools" : "Simplest tool found in web browser"
        "Burp Suite" : "Used for GET & POST based attacks"
        "curl" : "Can request web pages source code in terminal"
    }
]
```

~$what_is_port_scanning

"What is it": [
  {
    "Passive Attack" : "Network attack in which a system is monitored and scanned for open ports and vulnerabilities to connect or send data to discover hosts and services on a computer network by sending packets and analyzing the responses"
    "Ports" : "port is a number assigned to uniquely identify a connection endpoint and to direct data to a specific service"
    "Common Ports" : "80 / 443 - HTTP / HTTPS" "23 - Telnet" "22 - SSH" "21 - FTP" "3389 - RDP"
  }
],
"Format": [
  {
    "Nmap" : "Useful tool to achieve valuable results from port scan"
    "Netcat" : "Can take a passive attack and become active by connecting to servers or listen for reverse shell requests"
  }
]

```
┌──(kali㉿DESKTOP-7M5MDL7)-[~]
└─$ nmap --help
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
```

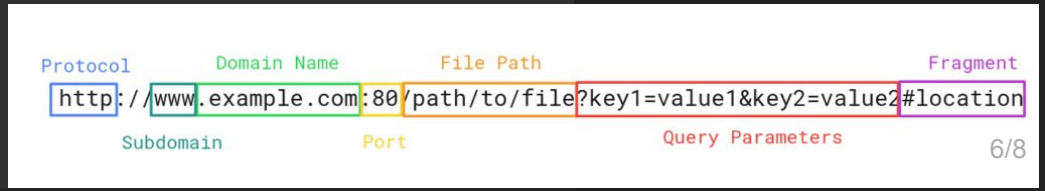
~$what_is_web_content_scanning

"What is it": [
  {
    "URL" : "the human readable address of a given unique resource on the web were each valid URL points to a unique IP, most interesting places for us will be in the subdomain or file paths"
    "Robots.txt" : "A file which tells search engine crawlers which URLs the crawler can access on your site, can be used to find useful file paths"
  }
],
"Format": [
  {
    "Dirb" : "dictionary based attack against a web server and analyzing the responses"
    "GoBuster" : " tool used to brute-force URIs including directories and files as well as DNS subdomains"

  }
]

```
# Nice try
# WW91J3JlIHRoZSBvbmUgY29uc3RhbnQgaW4gYSBzZWEgb2YgdmFyaWFibGVzLg==
User-Agent: *
Disallow: /confidential/
Allow: /
Allow: /resources
Allow: /events/
Allow: /about/
Allow: /code-of-conduct/

Sitemap: https://cybersoc.cf/sitemap.xml
```



~$what_is_hash_cracking

```
"What is it": [
    {
        "Hashes" :  "A one-way function that can be used to map data of arbitrary
        size to fixed-size values, useful form of storing / sharing secure content
        without revealing it"
        "Common" : {"MD5", "SHA-1", "SHA-256"}
        "Cracking" :  {"brute-force", "dictionary attacks", "combinator attacks",
        "mask attacks", "rule-based attack"}
    }
],
"Format": [
    {
        "John the ripper" : "Uses Brute Force attack and Dictionary Attack to
         crack password hashes"
        "Hashcat" : "Tool with numerous attack methods which include
         bruteforce using power of GPU
    }
]
```

```
┌──(kali㉿DESKTOP-7M5MDL7)-[~/Documents]
└─$ md5sum example_file.pdf
a14cbd80e149853eb58b0b31115e8a78  example_file.pdf

┌──(kali㉿DESKTOP-7M5MDL7)-[~/Documents]
└─$ sha256sum example_file.pdf
7aa1295428c9215ef7e357770805299e7afe9158029bd910cc6
309090a0abb3b  example_file.pdf
```

```
01dfae6e5d4d90d9892622325959afbe:7050461:hashcat

Session..........: hashcat
Status...........: Cracked
Hash.Name........: md5($pass.$salt)
Hash.Target......: 01dfae6e5d4d90d9892622325959afbe:7050461
Time.Started.....: Sat Sep 19 12:43:23 2020 (0 secs)
Time.Estimated...: Sat Sep 19 12:43:23 2020 (0 secs)
Guess.Base.......: File (passwordlist.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       35 H/s (0.04ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 9/9 (100.00%)
Rejected.........: 0/9 (0.00%)
Restore.Point....: 0/9 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: admin → azerty

Started: Sat Sep 19 12:42:41 2020
Stopped: Sat Sep 19 12:43:25 2020
kali@kali:~$
```

</SETTING YOU UP>

[what you will need]

- Kali Linux Virtual Machine -

- cybersoc{THIS_IS_YOUR_FIRST_FLAG} -

- ctf.cybersoc.cf -