

# Rentrée de Securimag

Aleknight

Securimag

Octobre 2020



Securimag

Que faisons nous ?

- Des présentations les jeudis soirs
- Des CTF (Capture The Flag)
- Des challenges entreprise
- GreHack
- D'autres trucs fun et cool



- Un événement d'envergure internationale
- Des conférences
- Des workshops
- Un CTF



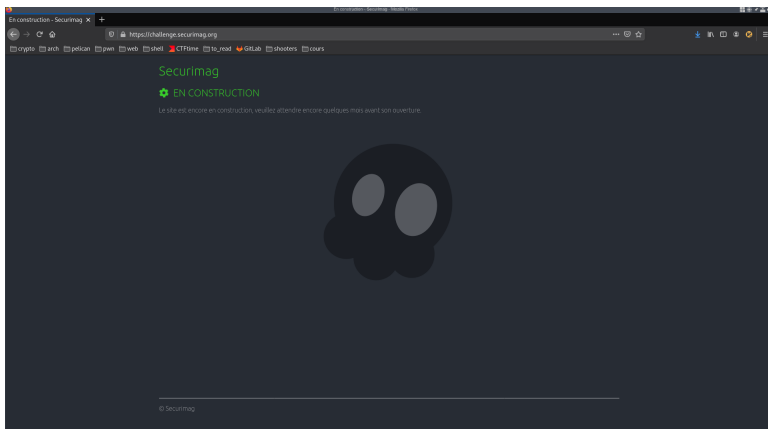
# Hacking

- Ethique
- Recherche
- Patience

Les différents domaines:

- Web
- Cryptographie
- Reverse Engineering
- Exploitation Logicielle
- Hardware
- Forensic
- Stéganographie





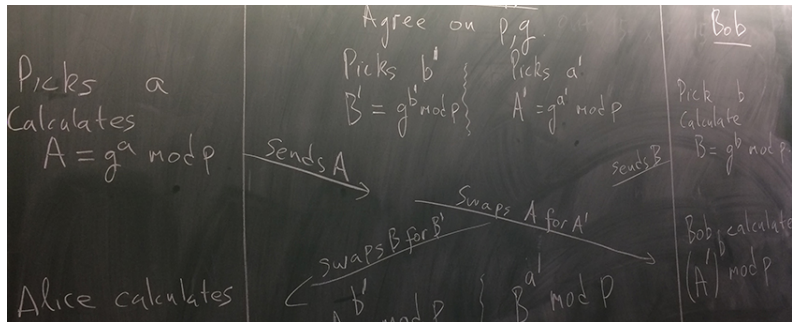
- Client
- Serveur

Quelques vulnérabilités:

- Local File Inclusion (LFI)
- SQL Injection (SQLi)
- Cross Site Scripting (XSS)



# Cryptographie



- Algorithmes connus
- Cryptanalyse

Quelques algorithmes connus:

- RSA (Asymétrique)
- AES (Symétrique)
- ECDSA (Signature)
- SHA3 (Hash)





# Reverse Engineering

```
00406770 - qt_metacall
undefined __thiscall qt_metacall(MainWindow * this, Call...
undefined Al:1 <RETURN>
MainWindow * RDI:8 (auto) this
Call ESI:4 param_1
int EDI:4 param_2
void * * RAX:8 param_3
undefined4 Stack[-0x1c]:4 local_1c
_MainWindow::qt_met...
MainWindow::qt_met...
---6770 PUSH R12
---6772 PUSH RBP
---6773 MOV R12,this
---6776 PUSH RAX
---6777 MOV RSP,param_3
---677a MOV EBX,param_1
---677c SUB RSP,0x10
---6780 CALL qt_metacall
---6785 TEST EAX,EAX
---6787 JS LAB_004067aa
```

```
00406789
---6789 TEST EAX,EAX
---678b JNZ LAB_004067b8
```

```
0040678d
---678d CMP EAX,0x9
---6790 JC LAB_004067a7
```

```
00406792
---6792 MOV param_1,EAX
---6794 MOV param_2,RBP
---6797 MOV this,r12
---679a MOV dword ptr [RSP + local_1c]...
---679e CALL MainWindow::qt_static_weta...
---67a3 MOV EAX,dword ptr [RSP + local_...
```

```
004067b8 - LAB_004067b8
LAB_004067b8
---67b8 CMP EAX,0xc
---67bb JNZ LAB_004067aa
```



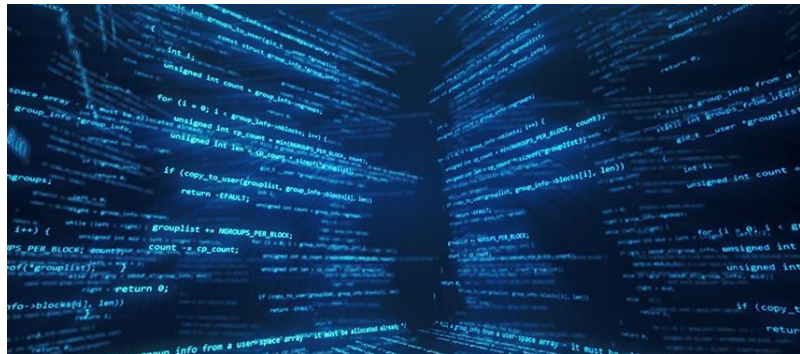
- Analyser un logiciel
- Comprendre le fonctionnement du logiciel étudié

Utilisation:

- Cracking (Illegal!!)
- Analyser des malwares
- Découvrir et exploiter des vulnérabilités



# Exploitation Logicielle



- Recherche de vulnérabilités et exploitation
- Détournement de l'exécution
- Elévation de privilèges

Des vulnérabilités:

- Buffer overflow
- Format String Bug
- Race condition

Des trucs qui en jettent:

- Exploitation de Browser web
- Exploitation de kernel (Linux, Windows, ...)



# Hardware



Securimag

Les différents domaines:

- Les divers bus de données
- Le monde de l'embarqué
- Le SDR (Software Defined Radio)

Des trucs vraiment cools:

- Lire et cloner des cartes d'accès dans votre poche
- Regarder la consommation électrique pour trouver une clé secrète
- Dumper le contenu de composants protégés



Capturing from wlp2s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-F> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1230	171.512644196	192.168.0.1	239.255.255.250	SSDP	312	NOTIFY * HTTP/1.1
1231	171.513195651	192.168.0.1	239.255.255.250	SSDP	367	NOTIFY * HTTP/1.1
1232	171.513752678	192.168.0.1	239.255.255.250	SSDP	377	NOTIFY * HTTP/1.1
1233	171.709705586	192.168.0.4	23.49.60.154	TCP	66	[TCP Keep-Alive] 34480 - 80 [ACK] Seq=382 Ack=914 Min=84128 Len=0 TSval=843731520 TSecr=...
1234	171.737277788	23.49.60.154	192.168.0.4	TCP	66	[TCP Keep-Alive ACK] 80 - 34480 [ACK] Seq=914 Ack=383 Win=30980 Len=0 TSval=4045868026 T...
1235	173.629717229	192.168.0.4	23.203.63.170	TCP	66	[TCP Dup ACK 240#16] 35438 - 80 [ACK] Seq=1 Ack=1 Min=501 Len=0 TSval=845687228 TSecr=61...
1236	173.629890663	192.168.0.4	23.203.63.170	TCP	66	[TCP Dup ACK 241#16] 35432 - 80 [ACK] Seq=1 Ack=1 Min=501 Len=0 TSval=845687227 TSecr=61...
1237	173.687806857	23.203.63.170	192.168.0.4	TCP	66	[TCP Dup ACK 242#16] [TCP ACKed unseen segment] 80 - 35438 [ACK] Seq=1 Ack=2 Min=243 Len...
1238	173.687806826	23.203.63.170	192.168.0.4	TCP	66	[TCP Dup ACK 243#16] [TCP ACKed unseen segment] 80 - 35432 [ACK] Seq=1 Ack=2 Min=243 Len...

▶ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

▶ Ethernet II, Src: D-LinkIn\_db:ee:43 (ec:ad:e0:db:ee:43), Dst: LiteonTe\_50:d2:65 (c8:ff:20:50:d2:65)

▶ Internet Protocol Version 4, Src: 5.9.259.164, Dst: 192.168.0.4

▶ Transmission Control Protocol, Src Port: 443, Dst Port: 39298, Seq: 1, Ack: 1, Len: 0

```
0000 c8 ff 20 50 d2 65 ec ad e0 db ee 43 80 00 45 00  --(Pre)---CSE
0010 00 34 04 e4 48 00 38 06 80 06 08 09 f0 a1 c9 a8  -4-@S...
0020 00 04 01 bb 99 82 28 b7 3a a3 68 80 64 0e 88 10  ....(:.hid...
0030 01 f9 05 02 00 00 01 01 08 0a 1d 18 ae 85 01 df  ...e.....
0040 b7 44  D
```

wlp2s0: <live capture in progress> Packets: 1238 - Displayed: 1238 (100.0%) Profile: Default



- Recherche des traces de malwares
- Analyse de dump mémoire
- Analyse de logs
- Recherche de fichiers





**SHAME!!!**



# A vous de jouer

Quelques liens utiles:

- **CTFd Securimag:** [ctf.securimag.org](https://ctf.securimag.org)
- Root-me: [root-me.org](https://root-me.org)
- Hack The Box: [hackthebox.eu](https://hackthebox.eu)
- Try Hack Me: [tryhackme.com](https://tryhackme.com)
- CryptoHack: [cryptohack.org](https://cryptohack.org)
- Newbie Contest: [newbiecontest.org](https://newbiecontest.org)



Merci de votre attention !

Questions ?



Securimag

**Time to Beer!!!**

