Lecture 2

Thursday, 17 November 2022 08:46

OWASP → cheat sheets for exploits & how to avoid them

top 10 → mandatory material (at least top 5)

XSS is a client-side injection

CWE : common weakness enumeration
↳ includes top 25 (less important)

insecure design : difficult / impossible to fix, since the entire system is flawed

market promotes a lack of attention being paid to cybersecurity

cookies have

value
domain
path
expiration date/time possibly: upon browser close
secure-only flag

first-party : cookie from this website
third-party : cookie from included resources
↳ when blocked : server will receive existing cookies, but cannot store new ones

search suggestions leak data for every letter typed

attack

1a. rent command and control server
1b. buy command and control software

2. gather intelligence

3. use exploit to get foot in the door

4. choose the right malware

watering hole → attack site user is likely to visit
spear phishing

malware initiates communication, to avoid firewall blocking communication
alternative : steal VPN credentials, then connect through VPN

many devices have weak authentication mechanisms on the local network

lateral movement : movement inside the network

can also move to physical attacks

browser exploitation framework:

fingerprinting (determine browser/OS/IP, use to target certain users)

RAT = remote administration tool

OSINT = open source intelligence gathering

targeted attack steps

1. reconnaissance
2. weaponization
3. delivery
4. exploitation
5. installation
6. command & control
7. action on objectives

an attack is direct if ...

examples: NAS (reachable from outside), router, USB attack, (D)DOS

opportunistic targeting : anyone can become a target