CS Games 2017

Security - Practical (70%)

Participants	2
Stations	1 Laptop
Total value	6%
Practical duration	2 hours 30 minutes
Theoretical duration	30 minutes

Comrades, the time has come.

Comrade Mao's writings have proven true: Western imperialism is taking our country hostage! The 20-year-old millionaire programmers heading these startups are causing an immeasurable embarrassment to the homeland because of their sense of innovation and speedy development of revolutionary products. We see ourselves forced to create a super-mega-secret unit that will allow us to go to cyber-war with these profit thirsty imperialist Americans!

Your mission is to infiltrate the servers of one of these American startups and exfiltrate specific information. The information will then be relayed to the politburo of the Central Committee of the Communist Party in order to obtain an economic advantage.

Rumor has it that a kiddie script exploited the site a few months ago and that a password dump is available online.

Your target: http://wtiiaas.csgames:YOUR_TEAMS_PORT/ (Written on your team's credential sheet)

In solidarity,

Tasks

The tasks are not necessarily in order. There are several ways to resolve certain tasks.

Several files are requested. Zip them together and submit this file.

Task	**Format**
Login through the Intranet Hint: only three user accounts are leverageable, system-wide	Intranet.txt: email:password of all leveraged accounts
Steal the CEO's session (obtain **all** of her cookies)	CEO-session.txt: cookies + proof of concept (payload, methodology, etc.)
Obtain a *premium* API key	Premium-key.txt: API key + simple proof of concept, short explanation (1-2 sentences)
Get remote code execution on the server	Code-exec.txt: simple proof of concept, short explanation (1-2 sentences)
Obtain the company's banking passwords (found in */home/sysadmin/banking.txt.pgp*). The file is encrypted, but it is possible to decrypt it.	- Banking.txt.pgp : Encryption file (half points) **OR** - Banking.txt: Decrypted file (all points) - banking-writeup.txt : Proof of concept + 1-2 sentences explaining your methodology
Some flags are hidden on the machine. Find them. Format: CSG-[a-zA-Z]+	Flags.txt: Flags + How/where you got them
Other	Other.txt: Add all vulnerabilities found **that were not previously documented** in prior challenges. IE if you found 4 SQL injections but only leveraged one to solve a challenge, document the 3 other SQLis here. (Proof of concept + 1-2 sentences per vulnerability)