CPTC Week 3 - Web / AI

Initial Setup

1. Set up GlobalProtect
    a. For CPP Students: Please see the VPN Instructions here
    b. For Non-CPP Students: Follow the instructions above using the username and password sent to you in order to log into the VPN.

Lab

Clone this week's Linux Pod through kamino.

- Kali credentials are `kali : kali`

If you're on mac, make sure you have this set up in your /etc/hosts

```
10.128.30.153   kamino.sdc.cpp
10.128.20.60    gonk.sdc.cpp
10.128.20.61    commando.sdc.cpp
10.128.20.62    gemini.sdc.cpp
10.128.20.63    godfrey.sdc.cpp
10.128.20.64    malenia.sdc.cpp
10.128.20.65    radahn.sdc.cpp
```

Once cloned, make sure to start both the Kali machine and the website machine.

Environment

There is one website located on 192.168.1.5, which will be the main target for this week.. Additionally, this week's assignment will include https://gandalf.lakera.ai/baseline for AI experience.

The router (192.168.1.1) is out of scope for this environment.

DM **@RedLeaf** if you need a hint or help with anything.

Deliverables

Find and exploit at least **3** web vulnerabilities and get to **level 7** of the Gandalf AI challenge, and submit a formal report. There are a total of 7 vulnerabilities I designed on the website.

Extra Credit will be given to those who fully find all vulnerabilities or any unintentional ones.

Within the report,
For the website, explain the following:

1. Explain the impact of the vulnerabilities to **technical** audiences
    a. Why did you give the vulnerability X impact/criticality rating? (Think likelihood and impact)
2. Include the steps taken to **enumerate** and **exploit** the vulnerabilities.
    a. Include **screenshots** for as many steps as possible, and **explain** the commands being used.
3. How would you remediate the vulnerability?

For the Gandalf AI Challenge:

1. Just include screenshots of your input and the response from the AI.